PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-243536
(43)Date of publication of application : 07.09.1999

(51)Int.Cl. H04N 7/16
H04H 1/00
H04L 9/08
H04L 9/32

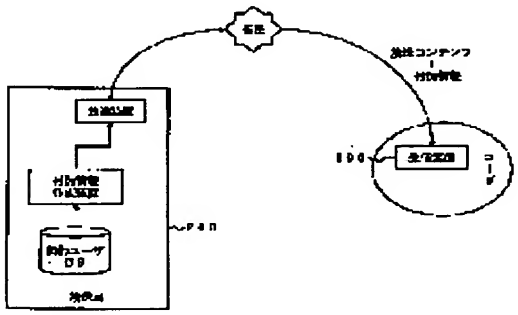
(21)Application number : 10-228287
(22)Date of filing : 12.08.1998

(71)Applicant : TOSHIBA CORP
(72)Inventor : AKIYAMA KOICHIRO
KAMIBAYASHI TATSU
TSUJIMOTO SHUICHI
ENDO NAOKI

(30)Priority
Priority number : 09366812 Priority date : 26.12.1997 Priority country : JP

(54) BROADCAST RECEIVER AND CONTRACT MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a broadcast receiver that realizes limited reception while keeping security of the same degree, even in the case that a broadcast band for transmission of information for limited reception is narrow and the number of subscribers have in creased to more than expected.
SOLUTION: This system has a master key in common to plural broadcast receivers 100 and a respective receiver ID set specifically to each broadcast receiver. In the case of receiving encrypted reception contract information including at least contract information and a receiver ID corresponding to the contact information, the master key is used to sequentially decode the encrypted reception contract information. The contract information, corresponding to the receiver ID in matching with the receiver IC possessed by the broadcast receiver, is selected and acquired among the decoded reception contract information, and the system determines whether or not a channel key for decoding the encrypted information contents is fed to a decoding section in order to decode the encrypted contents information, based on the acquired contract information.



LEGAL STATUS

[Date of request for examination] 26.02.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

THIS PAGE LEFT BLANK

the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3561154
[Date of registration]	04.06.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

THIS PAGE LEFT BLANK

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－243536

(43)公開日　平成11年(1999)９月７日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	7/16		Ｈ０４Ｎ	7/16	Ｚ
Ｈ０４Ｈ	1/00		Ｈ０４Ｈ	1/00	Ｆ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ
	9/32				６７１

審査請求　未請求　請求項の数21　ＯＬ　（全 52 頁）

(21)出願番号　特願平10－228287

(22)出願日　平成10年(1998)８月12日

(31)優先権主張番号　特願平9－366812

(32)優先日　平９(1997)12月26日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　秋山　浩一郎
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　辻本　修一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦　（外６名）

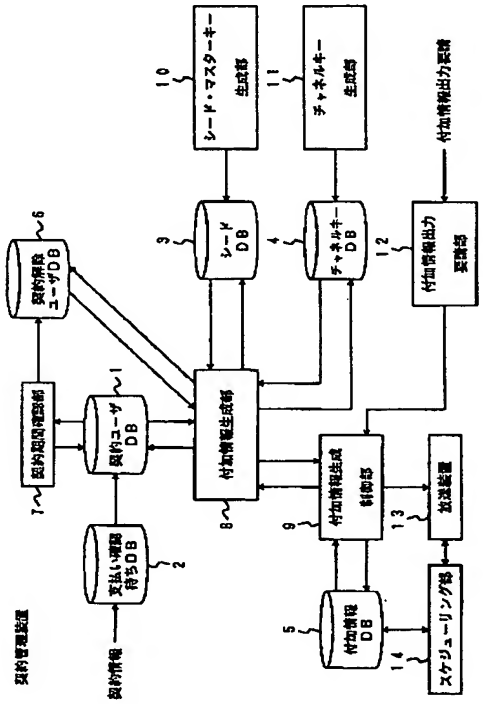
最終頁に続く

(54)【発明の名称】　放送受信装置および契約管理装置

(57)【要約】

【課題】限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる放送受信装置を提供する。

【解決手段】複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置ＩＤを持ち、少なくとも契約情報と該契約情報に対応した受信装置ＩＤを含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、該復号された受信契約情報のうち、本放送受信装置の有する受信装置ＩＤに一致する受信装置ＩＤに対応付けられた契約情報を選択して取得し、その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御する。



1

【特許請求の範囲】

【請求項１】　暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、
複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置ＩＤを持ち、
少なくとも前記契約情報と該契約情報に対応した受信装置ＩＤを含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、
該復号された受信契約情報のうち、本放送受信装置の有する受信装置ＩＤに一致する受信装置ＩＤに対応付けられた契約情報を選択して取得し、
その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする放送受信装置。

【請求項２】　前記チャネルキーは別途受信し、前記受信契約情報を受信しない限り、前記チャネルキーは前記復号部に送られることがないように制御することを特徴とする請求項１記載の放送受信装置。

【請求項３】　暗号化された前記チャネルキーを別途受信し、この暗号化されたチャネルキーを復号するチャネルキー復号鍵を含む前記受信契約情報を受信しない限り、前記チャネルキーが復号されないよう制御することを特徴とする請求項１記載の放送受信装置。

【請求項４】　前記チャネルキーの一部は別途受信され、前記チャネルキーの他の一部を含む前記受信契約情報を受信しない限り、前記チャネルキーが得られないように制御することを特徴とする請求項１記載の放送受信装置。

【請求項５】　前記チャネルキーは、前記受信契約情報に含まれて受信され、前記受信契約情報を受信しない限り、前記チャネルキーが得られないものであることを特徴とする請求項１記載の放送受信装置。

【請求項６】　暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、
前記暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、
を具備し、
前記マスター鍵を用いて、前記第１もしくは第２の受信手段で受信した暗号化されたチャネルキーを復号してチャネルキーを取得するとともに、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記契約情報を取得し、
その取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする請求項１記載の放送受信装置。

【請求項７】　暗号化されたコンテンツ情報を含む通常

2

放送波を受信する第１の受信手段と、
前記暗号化されたチャネルキーを復号するためのチャネルキー復号鍵を含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、
を具備し、
前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記チャネルキー復号鍵を取得し、
その取得したチャネルキー復号鍵を用いて、前記第１もしくは第２の受信手段で受信した暗号化チャネルキーを復号することによってチャネルキーを取得し、
前記取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする請求項１記載の放送受信装置。

【請求項８】　暗号化された放送コンテンツ情報と前記チャネルキーの一部を含む通常放送波を受信する第１の受信手段と、
前記チャネルキーの他の一部を含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段を具備し、
前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記チャネルキーの他の一部と前記契約情報を取得し、
前記第１の受信手段で受信したチャネルキーの一部と前記取得したチャネルキーの他の一部とからチャネルキーを再生し、
前記取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする請求項１記載の放送受信装置。

【請求項９】　暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、
前記チャネルキーを含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、
を具備し、
前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して該受信契約情報に含まれる契約情報とチャネルキーを取得し、
その取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報の復号部に送るか否か制御することを特徴とする請求項１記載の放送受信装置。

【請求項１０】　暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする請求項１記載の放送受信装置。

【請求項１１】　前記受信契約情報に含まれるデジタル

署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする請求項１記載の放送受信装置。

【請求項１２】　内部データをテスト出力するためのテスト制御部を具備し、

このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを制御することを特徴とする請求項１記載の放送受信装置。

【請求項１３】　暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダを具備したことを特徴とする請求項１記載の放送受信装置。

【請求項１４】　暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーは暗号化されたコンテンツ情報を復号するための復号部に送られることがないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、

少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、

前記チャネルキーは前記受信契約情報とは別途配信することを特徴とする契約管理装置。

【請求項１５】　暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するための暗号化されたチャネルキーが復号されないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、

少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報と前記暗号化されたチャネルキーを復号するためのチャネルキー復号鍵とを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする契約管理装置。

【請求項１６】　暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーが得られないように制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、

少なくとも放送受信装置毎個別に設定された受信装置ＩＤと、該受信装置ＩＤに対応した契約情報として前記チャネルキーの一部を含むものとを包含する受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して

送信し、

前記チャネルキーの他の一部を別途送信することを特徴とする契約管理装置。

【請求項１７】　暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーが得られないように、複数の放送受信装置を管理する契約管理装置であって、

少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報と前記チャネルキーとを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする契約管理装置。

【請求項１８】　カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする請求項１４～請求項１７のいずれか１つに記載の契約管理装置。

【請求項１９】　契約に変化の生じた契約者の受信契約情報を選択的に送信することを特徴とする請求項１４～請求項１７のいずれか１つに記載の契約管理装置。

【請求項２０】　前記受信契約情報に含まれる情報の種別に応じた識別子に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする請求項１～請求項１３のいずれか１つに記載の放送受信装置。

【請求項２１】　前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする請求項１４～請求項１７のいずれか１つに記載の契約管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、たとえば、契約内容（期間、視聴チャネル）に応じて放送配信されるコンテンツを復号する有料放送サービスのための契約管理装置およびこの契約管理装置にてコンテンツの復号が制御されるコンテンツの受信装置に関する。

【０００２】

【従来の技術】ディジタル放送は、通信衛星（ＣＳ）に始まって、ケーブルＴＶ、地上放送へとディジタル化が進むにつれ、いっそうのサービスの充実が期待されており、これからの放送サービスの主役をつとめていくものと思われる。

【０００３】ディジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャネル数の大幅な増加が可能となったことである。さらに、高度な誤り訂正技術が適用でるため、高品質で均質なサービスの提供が可能となる。

【０００４】放送のディジタル化により、多様な情報形態（映像、音声、文字、データ等）によるマルチメディアサービスの提供が可能となり、そのようなサービスを

5

提供するためのシステムも続々登場してきている。

【０００５】このようなシステムで、契約内容に基づいてスクランブルを解く、あるいは復号する有料放送サービスを提供する際、契約期間に即した顧客管理が行えなければいけない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャネルの番組の視聴を可能とするというものである。

【０００６】また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャネル、契約期間に即して）しかも確実に提供する必要がある。

【０００７】この意味で、従来は、放送受信装置毎にマスター鍵を用意し、受信契約している視聴者に対して受信契約しているチャネルのワークキーのみをマスター鍵で暗号化して送っていた。ここでワークキーはチャネル固有の鍵であり、暗号化されて送られてくる当該チャネルのチャネルキーを復号することができる。チャネルキーはスクランブルされた放送コンテンツをデスクランブルするのに用いられる。

【０００８】さらに、ワークキーは契約期間（通常１ヶ月）毎に設定され、その期間毎に放送局から送られて来る。このため契約期間毎各契約者に必要十分なワークキーを送らなくてはならない。だが逆に見ればワークキーが更新されることにより確実に契約期間が守られるという長所があった。しかし、このシステムを取る限り１ヶ月毎に全契約者に対してワークキーを放送波で送らなければならず、ＣＳ放送の契約者やチャネルが増加傾向にある今日送信量の観点からはかなり厳しくなりつつある。

【０００９】

【発明が解決しようとする課題】そこで、本発明は、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる放送受信装置、放送受信装置と放送送信装置（契約管理装置）を用いた限定受信システムを構築することを目的としている。

【００１０】

【課題を解決するための手段】（１）請求項１

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置ＩＤを持ち、少なくとも前記契約情報と該契約情報に対応した受信装置ＩＤを含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、該復号された受信契約情報のうち、本放送受信装置の有する受信装置ＩＤに一致する受信装置ＩＤに対応付けられた契約情報

6

を選択して取得し、その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【００１１】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる。例えば、契約期間に限って当該顧客のみに契約チャネルのコンテンツの視聴が可能となるような限定受信が行える。

【００１２】（２）請求項２：第２の実施形態（チャネルキーは、受信契約情報とは別途に配布）

請求項１記載の放送受信装置において、前記チャネルキーは別途受信し、前記受信契約情報を受信しない限り、前記チャネルキーは前記復号部に送られることがないように制御することを特徴とする。

【００１３】（３）請求項３：第３の実施形態（受信契約情報にチャネルキー復号鍵が含まれる）

請求項１記載の放送受信装置において、暗号化された前記チャネルキーを別途受信し、この暗号化されたチャネルキーを復号するチャネルキー復号鍵を含む前記受信契約情報を受信しない限り、前記チャネルキーが復号されないよう制御することを特徴とする。

【００１４】（４）請求項４：第１の実施形態（受信契約情報にチャネルキーの一部が含まれる）

請求項１記載の放送受信装置において、前記チャネルキーの一部は別途受信され、前記チャネルキーの他の一部を含む前記受信契約情報を受信しない限り、前記チャネルキーが得られないように制御することを特徴とする。

【００１５】（５）請求項５：第４の実施形態（受信契約情報にチャネルキーが含まれる）

請求項１記載の放送受信装置において、前記チャネルキーは、前記受信契約情報に含まれて受信され、前記受信契約情報を受信しない限り、前記チャネルキーが得られないものであることを特徴とする

（６）請求項６：第２の実施形態（チャネルキーは、受信契約情報とは別途に配布）

請求項１記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、前記暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、を具備し、前記マスター鍵を用いて、前記第１もしくは第２の受信手段で受信した暗号化されたチャネルキーを復号してチャネルキーを取得するとともに、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記契約情報を取得し、その取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【００１６】（７）請求項７：第３の実施形態（受信契約情報にチャネルキー復号鍵が含まれる）

請求項１記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、前記暗号化されたチャネルキーを復号するためのチャネルキー復号鍵を含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、を具備し、前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記チャネルキー復号鍵を取得し、その取得したチャネルキー復号鍵を用いて、前記第１もしくは第２の受信手段で受信した暗号化チャネルキーを復号することによってチャネルキーを取得し、前記取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【００１７】（８）請求項８：第１の実施形態（受信契約情報にチャネルキーの一部が含まれる）

請求項１記載の放送受信装置において、暗号化された放送コンテンツ情報と前記チャネルキーの一部を含む通常放送波を受信する第１の受信手段と、前記チャネルキーの他の一部を含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段を具備し、前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記チャネルキーの他の一部と前記契約情報を取得し、前記第１の受信手段で受信したチャネルキーの一部と前記取得したチャネルキーの他の一部とからチャネルキーを再生し、前記取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。

【００１８】（９）請求項９：第４の実施形態（受信契約情報にチャネルキーが含まれる）

請求項１記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、前記チャネルキーを含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、を具備し、前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して該受信契約情報に含まれる契約情報とチャネルキーを取得し、その取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報の復号部に送るか否か制御することを特徴とする。

（１０）請求項１～請求項９の記載の放送受信装置において、チャネルキー、マスター鍵の少なくとも一方が変更されることを特徴とする。

【００１９】鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。

（１１）請求項１、請求項３、請求項７記載の放送受信装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうちの少なくとも１つが変更されることを特徴とする。

【００２０】鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。

（１２）請求項１～請求項９の記載の放送受信装置において、チャネルキー、マスター鍵の少なくとも一方が変更され、チャネルキー、マスター鍵のそれぞれは、同時に最大２つの鍵を保持することを特徴とする。

（１３）請求項１～請求項９の記載の放送受信装置において、チャネルキー、マスター鍵の少なくとも一方が変更され、チャネルキー、マスター鍵のそれぞれにおいて同時に最大２つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。

（１４）請求項１、請求項３、請求項７記載の放送受信装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうちの少なくとも一つが変更され、チャネルキー、チャネルキー復号鍵、マスター鍵のそれぞれは、同時に最大２つの鍵を保持することを特徴とする。

（１５）請求項１、請求項３、請求項７記載の放送受信装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうちの少なくとも１つが変更され、チャネルキー、チャネルキー復号鍵、マスター鍵のそれぞれは、同時に最大２つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。

（１６）請求項１～請求項９の記載の放送受信装置において、チャネルキーは、チャネル毎に同時に最大２つ保持することを特徴とする。

【００２１】チャネルキーをチャネル毎に最大２つ保持することにより、チャネル切替時であっても（切替元にチャネルの受信契約を行っていれば）、保持している当該チャネルのチャネルキーを暗号化されたコンテンツ情報の復号部に即時的に送ることでチャネル切替の受信状態を良好にできる。

（１７）請求項１０

請求項１記載の放送受信装置において、暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報（例えば、チャネルキー等の鍵情報、受信契約情報）の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする。

（１８）請求項１０記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、その一部であることを特徴とする。

（１９）請求項１０記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、前記暗号化された必須情

報を該必須情報で再暗号化したもの、あるいは、数回再暗号化した情報のうち全部あるいは一部であることを特徴とする。

（２０）請求項１０記載の放送受信装置において、暗号化されていない必須情報（例えば、マスター鍵シード）の認証子は、該必須情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化したもの、あるいは、それをさらに圧縮したものを用いることを特徴とする。

（２１）請求項１１

請求項１記載の放送受信装置において、前記受信契約情報に含まれるデジタル署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする。

（２２）請求項１１記載の放送受信装置において、受信契約情報に当該放送受信装置に対する契約情報が含まれた時のみ、受信契約情報に含まれるデジタル署名を検証することを特徴とする。

（２３）請求項１１記載の放送受信装置において、デジタル署名検証用の公開鍵を変更することを特徴とする。

（２４）請求項１２

請求項１記載の放送受信装置において、内部データ（復号された受信契約情報、放送受信装置内の受信装置ＩＤ格納部に格納されている受信装置ＩＤ）をテスト出力するためのテスト制御部（スキャンパステスト用ラッチ部）を具備し、このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを制御することを特徴とする。

（２５）請求項１２記載の放送受信装置において、前記テスト制御部は、暗号化された内部データを出力することを特徴とする。

（２６）請求項１３

請求項１記載の放送受信装置において、暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダを具備したことを特徴とする。

（２７）請求項１３記載の放送受信装置において、前記カードリーダは、有効期間毎に複数の契約情報が記録された磁気カードから、前記複数の契約情報を読み出し、有効期間に応じてそれらの複数の契約情報を使い分けることを特徴とする。

（２８）契約管理装置

暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき放送配信される暗号化コンテンツ情報を復号することにより該コンテンツ情報を受信する複数の放送受信装置を管理する契約管理装置において、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【００２２】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（２９）請求項１４：第２の実施形態の契約管理装置

暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーは暗号化されたコンテンツ情報を復号するための復号部に送られることがないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャネルキーは前記受信契約情報とは別途配信することを特徴とする。

【００２３】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３０）請求項１５：第３の実施形態の契約管理装置

暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するための暗号化されたチャネルキーが復号されないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報と前記暗号化されたチャネルキーを復号するためのチャネルキー復号鍵とを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【００２４】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３１）請求項１６：第１の実施形態の契約管理装置

暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーが得られないように制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別

に設定された受信装置ＩＤと、該受信装置ＩＤに対応した契約情報として前記チャネルキーの一部を含むものとを包含する受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャネルキーの他の一部を別途送信することを特徴とする。

【００２５】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３２）請求項１７：第４の実施形態の契約管理装置

暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーが得られないように、複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報と前記チャネルキーとを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【００２６】本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３３）請求項１４～１５記載の契約管理装置において、チャネルキーおよびマスター鍵のうち少なくとも１つが予め定められた期間で変更されることを特徴とする。

（３４）請求項１４～１７記載の契約管理装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうち少なくとも１つが予め定められた期間で変更されることを特徴とする。

（３５）請求項１４～１７記載の契約管理装置において、前受信契約情報に対する認証子を受信契約情報に含めて送信することを特徴とする。

（３６）請求項１４～１７記載の契約管理装置において、前記受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報で前記契約情報を暗号化したもの、もしくは、その一部を用いることを特徴とする。

（３７）請求項１４～１７記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報を該鍵情報で暗号化したもの、前記暗号化された鍵情報を鍵情報で再暗号化したもの、もしくは数回再暗号化した情報のうち全部もしくは一部を用いることを特徴とする。

（３８）請求項１４～１７記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化し、必要があれば圧縮したものを用いることを特徴とする。

（３９）請求項１４～１７記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信することを特徴とする。

（４０）請求項１４～１７記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信し、デジタル署名検証用の公開鍵と作成用の秘密鍵のペアを生成する機構を具備し、一定期間で前記デジタル署名用の公開鍵と秘密鍵を変更すると共に、前記デジタル署名検証用の公開鍵を送信することを特徴とする。

（４１）請求項１８

請求項１４～１７に記載の契約管理装置において、カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする。

（４２）請求項１９

請求項１４～１７に記載の契約管理装置において、最近一定期間内に契約の変化の生じた（新規契約を含む）契約者の受信契約情報を選択的に送信することをことを特徴とする。

【００２７】契約の種類（例えば、契約変更、新規契約など）と契約後の経過期間によって、契約情報の放送頻度を変更するようにしてもよい。

（４２－１）請求項１４～１７に記載の契約管理装置において、契約の変化の生じた（新規契約を含む）時期により、受信契約情報の送信頻度を変化させることを特徴とする。

（４３）請求項２０

請求項１～請求項１３記載の放送受信装置において、前記受信契約情報に含まれる情報の種別に応じた識別子（情報識別子）に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする。

（４４）請求項２１

請求項１４～１７記載の契約管理装置において、前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする。

【００２８】

【発明の実施の形態】以下、本発明の実施形態について図面を参照して説明する。

【００２９】（第１の実施形態）

１）放送システムの概略

図１は、本発明の契約管理装置および放送受信装置を用いた放送システムの概略構成を示したもので、放送局２００から衛星を利用して受信契約を行った各ユーザにコンテンツを提供するサービス形態の場合を示している。なお、図１では衛星放送の場合を例にとり説明するが、地上波にてコンテンツを提供するサービス形態の場合も

同様である。

【００３０】図２は、図１に示した放送サービスへの加入・継続契約時、契約更新時、解約時、課金手続きの概略的に流れを示したものである。

【００３１】図２に示すように、図１の放送サービスへの加入を希望するユーザは、加入手続きを代行する所定の代理店にて、視聴を希望するチャネル、視聴期間等の契約内容に伴った所定の加入手続きを行う。代理店を介して、その契約内容が放送局側の契約ユーザデータベースに登録されると、その登録内容に従ったユーザへのサービス提供を開始する。このサービス提供に対してユーザが支払うべき料金を例えばクレジットカード、あるいは銀行を介しての支払うようにしてもよい。

【００３２】ユーザへのサービス提供は、もっぱら、放送局側にある契約者データベースの登録内容に従ったものである。従って、加入時の契約内容の継続・更新、解約時等には、ユーザによる直接あるいは所定の代理店等を介してのその旨の通告を受けて、契約ユーザデータベースの登録内容を更新あるいは消去すればよい。なお、放送局は、加入料、受信料等の支払を確認した上で、当該ユーザへのサービス提供を開始あるいは継続するようにしてもよい。

【００３３】２）契約管理装置

（１）図３は、本実施形態に係る契約管理装置の構成例を示したもので、図１の放送局２００に設置されて用いられる。

【００３４】放送局２００では、チャネル毎に予め定められたチャネルキーＫｃｈによって暗号化したコンテンツ情報（［コンテンツ］Ｋｃｈ）、端末ＩＤおよびチャネルキーＫｃｈ等を含む付加情報をマスターキーＫｍによって暗号化した付加情報（［付加情報］Ｋｍ）を放送する。

【００３５】付加情報は放送受信契約し、受信料を支払ったユーザのみに受信許可を与えるためのもので、各ユーザ宅に設置された受信装置は受信装置自身の持つマスターキーＫｍによって受信された暗号化付加情報（［付加情報］Ｋｍ）を復号し、その中に含まれる端末ＩＤと受信装置のもつ端末ＩＤとを比較し、一致していた場合には、そこに含まれているチャネルキーＫｃｈを受信装置の持つデータベースに格納し、暗号化されたコンテンツ情報（［コンテンツ］Ｋｃｈ）を復号するためにこれを用いる。

【００３６】チャネルキーＫｃｈは一定の期間（例えば１ヶ月）毎に変更され、契約期間が切れたユーザにはそれ以降の付加情報は送られず、対応するチャネルキーＫｃｈが入手できないことから視聴できないことになる。

【００３７】さらに、この方式の安全性を向上させるため、マスターキーＫｍを一定期間毎に更新する。これは受信装置と放送装置の両方に共通にある乱数発生器を用いて行ない、放送波ではその乱数発生器に乱数を発生させる初期値（以下シードという）を受信装置に定期的に送る。これにより、たとえマスターキーＫｍが露見しても、一定期間しかそれが有効でないので、不正視聴を防止することが可能となる。また、復号鍵そのものを配信するのではなく、復号鍵を生成するために基となる情報を配信するので、セキュリティ性が高い。

【００３８】さて、図３の契約管理装置は、付加情報の生成と、その生成された付加情報をマスターキーＫｍで暗号化して放送するためのものである。

【００３９】まず、図７に示すフローチャートと図３を参照して、契約ユーザＤＢ１の登録処理動作について説明する。図１の放送サービスへの加入を希望するユーザとの間で、放送契約がなされると、図３の契約管理装置に契約情報が入力され（ステップＳ１）、支払い確認待ちデータベース（ＤＢ）２に蓄えられる（ステップＳ２～ステップＳ３）。支払い確認待ちＤＢ２において支払確認が済んだ項目から順次契約ユーザデータベース（ＤＢ）１に送られ、支払い確認待ちＤＢ２からは消去される（ステップＳ２～ステップＳ４）。

【００４０】契約ユーザＤＢ１には、図４に示す形式でデータが蓄えられる。図４において受信端末ＩＤは受信端末を特定するための情報であり、チャネル番号は契約済みのチャネルの番号である。契約期間は契約済みの期間（例えば１９９８年０１月３１日までなど）が予め定められた形式で記入されている。

【００４１】契約期間は契約期間確認部７で一定のタイミングでその有効性を確認する。ここで無効とされた場合は契約解除ユーザデータベース（ＤＢ）６に当該契約情報を送り、契約ユーザＤＢ１からは削除する。従って、契約期間の経過した（契約切れ）のユーザに関する情報は、契約ユーザＤＢ１から消去されているため、付加情報は配信されない。

【００４２】シードデータベース（ＤＢ）３は、シード・マスターキー生成部１０が一定のタイミングで生成したマスターキー生成用のシードから生成されるマスターキーをそのシードＩＤ及び有効期限とともに、図５に示す形式で格納している。

【００４３】チャネルキーデータベース（ＤＢ）４は、チャネルキー生成部１１が一定のタイミングで生成したチャネルキーをチャネル番号、チャネルキーＩＤやその有効期限とともに図６に示す形式で格納している。

【００４４】次に、契約ユーザ毎に対応した付加情報を生成し、これを放送装置１３を使って受信装置に送る手順を図８に示すフローチャートを参照して説明する。

【００４５】付加情報生成制御部９は、付加情報生成部８に対し、付加情報生成の指示を送る（ステップＳ１１）。この指示とは、例えば「１９９７年１２月１日から１ヶ月間契約している契約ユーザの付加情報を送れ」なる内容のもので、予め定められた形式のビット列で表現されたものでもよい。このような指示が出されると付

加情報生成部８では契約ユーザＤＢ１から１９９７年１２月１日から少なくとも１ヶ月間契約しているユーザの情報を検索して、当該情報を読み込む（ステップＳ１２～ステップＳ１３）。契約ユーザＤＢ１から読み込まれたユーザ情報（図４参照）から各ユーザの端末ＩＤ、チャネル番号を得る（ステップＳ１４）。

【００４６】ここで、契約期間の最小単位は１ヶ月で、契約有効期限は１日にはじまり月末に終了するとし、チャネルキーもこの契約最小期間に固有なものとする。すなわち、１１月のチャネルキーは１２月のそれとは異なるものを用い、それぞれの月内では変更しないものとする。また、当然チャネル番号が異なれば期間が同じでも違うチャネルキーを使うものとする。

【００４７】次に、付加情報生成部８は、チャネルキーＤＢ４から１９９７年１２月１日から１９９７年１２月３１日に有効なチャネルキーＫｃｈを検索して、当該チャネルキーＫｃｈ読み込む（ステップＳ１５）。また、シードＤＢ３から１９９７年１２月１日から１９９７年１２月３１日に有効なシードに対応したマスターキーＫｍを検索し、当該マスターキーＫｍを読み込む（ステップＳ１６）。ここでもマスターキーの切り替えの最小単位は 1ヶ月とする。ただマスターキーの場合その性格上必ずしも 1ヶ月で切り替える必要はない。

【００４８】以上によって得られた情報（各ユーザの端末ＩＤ、契約チャネル番号、チャネルキーＫｃｈ）をもとに、付加情報生成部８では、図９（ｂ）に示すような各ユーザ毎の付加情報を生成し、マスターキーＫｍで暗号化する（ステップＳ１７）。ここで生成された各契約ユーザ毎の暗号化付加情報は順次付加情報生成制御部９、放送装置１３に送られる。

【００４９】放送装置は、暗号化付加情報を所定の周波数帯域の放送波に変換して各受信装置に向けて配信する（ステップＳ１８）。

【００５０】一方、各チャネル番号に対応するチャネルキーＫｃｈを用いて暗号化された暗号化コンテンツ情報（図９（ａ）参照）は、この付加情報とは別途（別の帯域で）送られ、受信装置ではその両方を受信するようになっている。

【００５１】図１０は、暗号化コンテンツ情報の生成および配信（放送）するための放送局２００に設置されるコンテンツ情報の配信装置の構成例を示したものである。なお、図１０において、図３と同一部分には同一符号を付している。

【００５２】各チャネルのコンテンツ情報は、図１０に示すように、コンテンツ情報データベース（ＤＢ）２１に蓄積されている。暗号化部２２は、コンテンツ情報ＤＢ２１から各チャネル番号に対応したコンテンツ情報を読み出すとともに、チャネルキーＤＢ４から先ほどの付加情報生成範囲で有効なチャネル番号毎のチャネルキーを読み出して、各チャネルのコンテンツ情報を当該チャネル番号のチャネルキーＫｃｈで暗号化し、情報付加部２３に送る。

【００５３】マスターキーＫｍを一定期間毎に更新する場合、情報付加部２３では、シードＤＢ３から先ほどの付加情報生成範囲で有効なマスターキーシードあるいはシードＩＤを読み出し、それを放送装置１３へ出力する。

【００５４】放送装置１３では、チャネルキーで暗号化されたコンテンツ情報およびマスターキーシードあるいはシードＩＤを多重して、所定の周波数帯域の放送波に変換して各受信装置に向けて配信する。

【００５５】ユーザ毎チャネル毎の付加情報を個別に送るため大量の情報を配信する必要が生じ、一度に全ての情報を送れない場合は付加情報生成部８で生成された付加情報を一旦付加情報データベース（ＤＢ）５に蓄えておき、そこから配信する部分を取り出して放送配信し、配信が終了した後、該付加情報ＤＢ５から消去するとしてもよい。あるいは、付加情報生成制御部９が付加情報の生成をコントロールし、配信できる範囲のものだけを付加情報生成部８に指示してもよい。

【００５６】また、１回の放送だけでは受信装置が（何らかの理由で）受信できないこともある。このため、付加情報は契約期間の前から（可能な限り）何度も頻繁に送る必要がある。しかしそれでも（長期間受信不能なところに受信装置が存在するなどの理由で）受信できない場合もあるであろう。この場合、ユーザは視聴できなくなるので、ユーザからのクレームという形で放送局側にフィードバックがかかる。その際は、付加情報出力要請部１２に端末ＩＤと該当チャネル番号を含む付加情報出力要請信号を送り、付加情報出力要請部１２は付加情報生成制御部９にそれを送り、付加情報生成制御部９では契約ユーザＤＢ１を検索し、有効な契約を確認したら前述の手続きに従って暗号化した付加情報を生成し、放送する。

【００５７】（２）なお、上記説明では、付加情報にチャネルキーＫｃｈそのものを含む場合について説明したが、この場合に限らず、チャネルキーＫｃｈを例えば上位数十ビットと残りの下位数十ビットとの２つのチャネルサブキーＨ、Ｌに分割して、一方のチャネルサブキーＨのみを付加情報に乗せ、他方のチャネルサブキーＬをチャネルサブキーＫｃｈにて暗号化されたコンテンツ情報に付加（あるいは多重）して配信するようにしてもよい。

【００５８】この場合の契約管理装置の付加情報生成部８では、チャネルキーＤＢ４から付加情報の生成範囲で有効なチャネルキーからチャネルサブキーＨを抽出して、ユーザの端末ＩＤ、契約チャネル番号、チャネルサブキーＨをもとに、図１１（ｂ）に示すような各ユーザ毎の付加情報を生成し、マスターキーＫｍで暗号化する。

【００５９】また、図１０に示したコンテンツ情報の配信装置の情報付加部２３では、さらに、チャネルキーＤＢ４から先ほどの付加情報生成範囲で有効なチャネル番号毎のチャネルキーからチャネルサブキーＬを抽出して、放送装置１３へ出力する。放送装置１３からは、図１１（ａ）に示すように、チャネルキーで暗号化されたコンテンツ情報、チャネルサブキーＬ、さらに必要に応じてマスターキーシードあるいはシードＩＤが多重された所定の周波数帯域の放送波が各受信装置に向けて配信される。

【００６０】（３）付加情報として、図１２に示すような各契約ユーザ固有の付加情報（端末付加情報）と、図１３に示すようなチャネル番号に対応したチャネル付加情報とを用いる場合を考える。

【００６１】図１２に示すように端末付加情報は、端末ＩＤ及びチャネル番号と、当該端末ＩＤにて識別される受信装置との契約が有効／無効を示す情報とから構成されている。これは端末付加情報に記載された端末ＩＤを自身の端末ＩＤとして持つ受信装置の受信契約が、同じく端末付加情報の記載されたチャネル番号のチャネルで有効か無効かを示すものである。

【００６２】端末付加情報を考えるとき、受信装置は、当該チャネルの受信契約が有効であるという端末付加情報（以下、有効の端末付加情報あるいはＯＮ信号と呼ぶ場合がある）が来たら、それ以降当該チャネルを無効とする端末付加情報（以下、無効の端末付加情報あるいはＯＦＦ信号と呼ぶことがある）が来るまで当該チャネルは有効とし、逆に当該チャネルの無効の端末付加情報が来たら、それ以降当該チャネルの有効の端末付加情報が来るまで当該チャネルを無効にする。

【００６３】端末付加情報はチャネルキーを含まないので全体のサイズを半分以下に減らせる特徴がある。すなわち、チャネルキーで暗号化されたコンテンツの解読を防ぐため、チャネルキーを最低限でも５６ｂｉｔ程度必要となる一方、チャネルキー以外の端末ＩＤやチャネル番号等の情報は３０ｂｉｔ程度でも十分である。従って、付加情報にチャネルキーを含めた場合、付加情報全体に対するチャネルキーの占める割合が大きくなってしまう。しかし、付加情報からチャネルキーを除くことにより、付加情報全体のサイズが半分以下になる。このため、前述の方式よりも小さな付加情報を送ることになるため、単位時間あたりに送れる付加情報の数が増える。そればかりか、各ユーザ宛にチャネルキーの切替時に同期して、例えば、１ヶ月毎に個別にチャネルキーを送る必要がなく、端末付加情報を配信するのは新規契約時と契約切れの時のみであるから配信する全体の付加情報の量は激減する。

【００６４】実際、この場合、ユーザ個別に配信する端末付加情報は、放送受信を有効にする時と無効にする時に配信すれば良いだけなので通常の場合、極めて少なくて済む。

【００６５】図１２に示したような端末付加情報を配信する契約管理装置の構成は、図３と同様で動作が異なる。すなわち、付加情報生成部８は、端末付加情報を作成する際、チャネルキーＤＢ４を検索せずに、契約ユーザＤＢ１とシードＤＢ３と契約解除ユーザＤＢ６の情報を検索して端末付加情報を作成するようになっている。これは、チャネルキーを端末付加情報に含める必要がない一方、契約解除をしたユーザに対しては端末付加情報を送らなければならないためである。

【００６６】図３の契約管理装置の処理動作について説明する。

【００６７】契約情報が入力されて契約ユーザＤＢ１へ登録処理は、図７のフローチャートに従って実行される。

【００６８】付加情報生成制御部９は、付加情報生成部８を介して予め定められたタイミングで契約ユーザＤＢ１に登録されている新規契約ユーザの情報を検索する。付加情報生成部８では、検索された新規契約ユーザの情報から端末ＩＤと契約チャネル番号を抽出し、図１２に示したような端末付加情報を作成する（この場合は契約を有効にするのであるから有効の端末付加情報を作成する）。

【００６９】更に、付加情報生成部８は、シードＤＢ３を検索して、現在有効なマスターキーを抽出する。このマスターキーを使って先に生成された端末付加情報を暗号化し、付加情報生成制御部９に送る。

【００７０】付加情報生成制御部９では、これを放送装置１３に送り、予め定められた帯域で放送する。

【００７１】ここで、配信すべき端末付加情報が多すぎて一時に放送できないこともあるであろう。そのときは生成された暗号化された端末付加情報を付加情報ＤＢ５に一時的に蓄えるよう付加情報生成制御部９が制御することも可能である。

【００７２】契約ユーザ側では、ユーザ自身の持つ受信装置にて、図１２に示したような端末付加情報を受信すると、受信装置内部の復号ユニット（後述）にて、これを復号して契約が有効であるか否かが確認される。有効である旨が記述されていたときに、当該チャネルのチャネルキーを用いて、例えば付加情報とは別帯域で配信されてくる当該チャネルのコンテンツ情報を復号して、ユーザは所望の番組を視聴することができるようになる。

【００７３】契約期間確認部７は、予め定められたタイミングで契約ユーザＤＢ１を検索し、契約切れのユーザを検索する。検索された契約切れのユーザに関する情報は、契約解除ユーザＤＢ６に登録する。

【００７４】契約切れのユーザに対しては、無効の端末付加情報を配信する必要がある。そこで、付加情報生成制御部９は、前述の有効の端末付加情報を配信するときと同様、まず、付加情報生成部８を介して予め定められ

たタイミングで契約ユーザＤＢ１に登録されている新規契約ユーザの情報を検索する。

【００７５】付加情報生成部８では、検索された新規契約ユーザの情報から端末ＩＤと契約チャネル番号を抽出し、図１２に示したような端末付加情報を作成する（この場合は契約を無効にするのであるから無効の端末付加情報を作成する）。更に、付加情報生成部８は、シードＤＢ３を検索して、現在有効なマスターキーを抽出する。このマスターキーを使って先に生成された端末付加情報を暗号化し、付加情報生成制御部９に送る。付加情報生成制御部９では、これを放送装置１３に送り、予め定められた帯域で放送する。

【００７６】ここで、無効の端末付加情報を配信する場合は、１度放送するだけでは（何らかの原因で）受信装置が確実に受信できない場合もあり、例えば、１度発信した情報を何ヶ月かに渡って定期的に流すようにする必要がある。さもないと当該受信装置は永久的に視聴可能な状態になってしまい、受信契約を管理しているとは言えない状態に陥る。このことは、有効の端末付加情報を送る場合でも同様だが、この場合はユーザからのクレームによって未受信が検出され、付加情報出力要請部１２を用いて、当該未受信の有効の端末付加情報を配信することもできるので、無効の端末付加情報を配信する場合ほど長い間流し続けなくてもよい。

【００７７】次に、コンテンツ情報を復号するためのチャネルキーの配信について説明する。

【００７８】今、チャネルキーを１ヶ月に１度変更するとして、これを図１３に示すようなフォーマットでチャネル番号、必要に応じてチャネルキーＩＤとともにチャネル付加情報として生成し、その時点で有効なマスターキーにて暗号化する。この暗号化されたチャネル付加情報を所定のタイミングで端末付加情報を送るのと同じ帯域で配信する。

【００７９】配信時に、端末付加情報とチャネル付加情報とを区別するための例えばビット情報を、端末付加情報とチャネル付加情報との暗号化されていない部分に付けておけばよい。

【００８０】受信装置側では、該ビット情報をチェックして、チャネル付加情報である場合には、それを復号し、さらにチャネル付加情報に含まれるチャネル番号をチェックして、現在受信契約しているチャネル番号であれば、該チャネル付加情報に含まれるチャネルキーＩＤおよびチャネルキーを格納する処理を行なう。

【００８１】ここで、チャネルキーを変更する場合、実際にチャネルキーを変更する時点よりも前に、変更するチャネルキーを配信するのが望ましい。これにより、受信装置側ではチャネルキーの変更に伴うコンテンツ情報の復号が連続して行える。例えば、１９９８年１月１日から切り替わるチャネルキーのチャネル付加情報は１９９７年１２月１５日から送るようにすれば、１６日間の間に受信装置が当該チャネルキーのチャネル付加情報を受信する可能性は極めて高くなり、それを受信装置の所定のデータベースに格納しておけば、１９９７年１２月３１日から１９９８年１月１日の間のチャネルキーの切替えがスムーズに行え、ユーザは、連続的に所望のチャネルの番組を視聴することが可能となる。

【００８２】一方、新規契約したユーザの受信装置には（今まで受信契約していなかったのであるから）当該チャネルキーが格納されていない。このため新規契約ユーザは契約後すぐには視聴できないという問題がある。この問題を解決するためには、チャネル付加情報を頻繁に配信する必要がある。しかし、図１３に示したようなチャネル付加情報は、各ユーザ個別のものではなく、チャネル番号に対応したものであるので（すなわち、各ユーザに共通して配信すべき情報であるので）、各ユーザ個別に配信する必要のある図９（ｂ）に示したえような付加情報の場合と比較して、配信量は少なくてすむので、チャネル付加情報を頻繁に送ることは十分に可能である。

【００８３】なお、チャネル付加情報の配信は、チャネルキー変更直前（１９９７年１２月３１日）と直後（１９９８年１月１日）には普段より頻繁に送るようにすると効果的である。何故ならば、これらの期間には確実に受信して欲しいからである。同様のことは受信契約の更新時期（新規受信契約開始の時期や契約切れの時期）にも言える。

【００８４】前述の（１）の説明では、チャネルキーの切り替えをもって、同時に契約の切り替え（契約切れ／継続契約）を意味していたので、チャネルキーの切替時と契約切替時とを同じ時期にしていたが、有効／無効の端末付加情報を用いる場合は、必ずしも同じ時期にする必要がない。

【００８５】このように、有効／無効の端末付加情報とチャネル付加情報とを用いる場合、契約ユーザに配信すべき付加情報の内容を各ユーザ個別の情報とユーザ共通の情報とにわけ、契約切替時期には端末付加情報を頻繁に配信し、チャネルキーの切替時期にはチャネル付加情報を頻繁に配信すればよいので、配信量の分散が図れる。

【００８６】（４）上記（３）の説明では、有効／無効の付加情報を配信することにより、受信装置のコンテンツ情報の復号の可否を制御（新規契約時と契約切れ時の受信端末への制御）するものであった。これと同様の操作を、例えば、図９（ｂ）に示す付加情報を用いても行うことができる。

【００８７】すなわち、契約期間中は、付加情報生成部８は、図９（ｂ）に示すような端末ＩＤ、チャネルキー、チャネル番号を含む付加情報を生成して各ユーザ宛に配信するが、例えば１ヶ月（チャネルキーの有効期間であると同時に契約期間の最小単位でもある期間）毎

に、契約契約解除ユーザＤＢ６を検索して、契約の切れたユーザに対しては、チャネルキーを含まない付加情報を生成して配信するようにする。当該受信装置では（有効なチャネルキーを受け取ることがないので）、以後コンテンツ情報の復号はできない。このように、チャネルキーを含まない付加情報は、当該ユーザの受信装置に対し契約切れの旨を通知するとともに、当該受信装置での視聴を不可能とするための制御信号でもある。

【００８８】図１１（ｂ）に示したようなチャネルサブキーＨを含む付加情報を用いる場合も同様で、契約期間中は、付加情報生成部８は、図１１（ｂ）に示すような端末ＩＤ、チャネルサブキーＨ、チャネル番号を含む付加情報を生成して各ユーザ宛に配信するが、例えば１ヶ月（チャネルキーの有効期間であると同時に契約期間の最小単位でもある期間）毎に、契約契約解除ユーザＤＢ６を検索して、契約の切れたユーザに対しては、チャネルサブキーを含まない付加情報を生成して配信するようにする。当該受信装置では（チャネルキーを生成するために必要なチャネルサブキーを入手できないので）、以後コンテンツ情報の復号はできない。このように、チャネルサブキーを含まない付加情報は、当該ユーザの受信装置に対し契約切れの旨を通知するとともに、当該受信装置での視聴を不可能とするための制御信号でもある。

【００８９】（５）次に、図３に示す契約管理装置のスケジューリング部１４について説明する。

【００９０】スケジューリング部１４は、付加情報ＤＢ５に格納された付加情報を配信する際、および、放送装置１３にて付加情報を配信する際に、各ユーザ側の受信装置にて確実に付加情報が受信されるように配信制御を行うものである。

【００９１】すなわち、例えば、受信契約後、契約変更時、契約解約時、チャネルキー等の更新時には付加情報を頻繁に送る必要があり、そのための付加情報の配信スケジューリングに従って、付加情報の配信制御を行うのが、スケジューリング部１４である。

【００９２】付加情報の配信スケジューリングとして、視聴率の高い番組が放送される時間帯に頻繁に送ることも付加情報をユーザ側に確実に配信する上で有効な手段である。

【００９３】３）受信装置

（１）図１４は、本実施形態に係る受信装置１００の構成例を示したもので、前述の図３に示したような放送局側に設置されている契約管理装置で生成された付加情報および図１０に示したようなコンテンツ情報の配信装置から出力される放送波を受信するためのものである。

【００９４】ここで図１４に示した受信装置１００にて受信される放送波には、次のような情報が含まれているものとする。

・　マスターキーシード
・　［付加情報］Ｋｍ　…付加情報をマスターキーＫｍで暗号化したもの
・　チャネルサブキーＬ
・　［コンテンツ］Ｋｃｈ　…コンテンツ情報をチャネルキーＫｃｈで暗号化したもの

マスターキーシードは、図１４の受信装置１００のマスターキー生成部５０４がマスターキーを生成する元になるデータである。

【００９５】チャネルサブキーＬは、付加情報に含まれるチャネルサブキーＨと合わせて、チャネルキーＫｃｈを生成するための情報である。

【００９６】なお、チャネルサブキーＬを放送波に多重化して配信しない場合もある。この場合、チャネルキーＫｃｈ＝チャネルサブキーＨとなる。

【００９７】付加情報は、次のような情報が含まれているものとする。

・　端末ＩＤ　…受信装置の識別情報
・　チャネル番号（複数も可）
・　チャネルサブキーＨ

端末ＩＤにて識別される受信装置との間で契約されているチャネルが１つのみの場合は、チャネル番号を必ずしも含む必要はない。また、チャネルサブキーＨが含まれないことがある。

【００９８】付加情報にチャネルサブキーＨが含まれる場合、当該付加情報は、当該端末ＩＤにて識別される受信装置が当該チャネルを視聴する事を可能にする、いわゆるＯＮ信号である。

【００９９】一方、付加情報にチャネルサブキーＨが含まれない場合、当該付加情報は、当該端末ＩＤにて識別される受信装置が当該チャネルを使用することを禁止する、いわゆるＯＦＦ信号となる。

【０１００】前述の契約管理装置にて生成されて配信された付加情報を受信した図１４の受信装置における契約管理のメカニズムの概要を述べる。

【０１０１】付加情報がチャネルサブキーＨを含む場合、復号ユニット１１０は、付加情報から抽出されたチャネルサブキーＨをチャネルサブキー格納部５０８に格納する。従って、チャネルデコーダ５０９は、チャネルサブキー格納部５０８からチャネルサブキーＨを取得し、放送波に多重化して配信されるチャネルサブキーＬと合わせて、チャネルキーＫｃｈを生成することができる。そして、生成したチャネルキーＫｃｈを用いて、当該チャネルのコンテンツ情報を正しく復号することができる。

【０１０２】付加情報に含まれる端末ＩＤと、受信装置に予め与えられているＩＤとが一致しない場合、復号ユニット１１０はチャネルサブキーＨをチャネルサブキー格納部５０８に格納しない。

【０１０３】放送局２００の契約管理装置は、契約済みの受信装置のＩＤとその際契約された視聴チャネルの番号および当該チャネルのチャネルサブキーＨを含む付加

情報を放送波に多重化して放送することによって、当該契約受信装置のみに、契約チャネルの視聴を開始させることができる。

【０１０４】付加情報がチャネルサブキーＨを含まない場合、復号ユニット１１０は、チャネルサブキー格納部５０８に対してチャネルサブキーＨの消去指示を出力する。当該チャネルのコンテンツ情報はチャネルキーＫｃｈによって暗号化されている。チャネルデコーダ５０９は、チャネルサブキーＨを取得できず、従って、コンテンツ情報に多重化して配信されるチャネルサブキーＬと合わせて、チャネルキーＫｃｈを生成することができない。すなわち、当該チャネルのコンテンツ情報を復号することができないため再生が行われない。

【０１０５】放送局２００の契約管理装置は、解約受信装置のＩＤと解約チャネル番号を含み、かつチャネルサブキーＨを含まない付加情報を、放送波に多重化して放送する。これによって、当該解約受信装置のみに、契約チャネルの視聴を禁止（すなわち、解約）することができる。

【０１０６】次に、図１４の受信装置の処理動作を図１５～図１８に示すフローチャートを参照して、より詳細に説明する。

【０１０７】まず、受信部５０１が放送波を受信すると、Ａ／Ｄ変換部５０２がディジタル信号に変換するとともに、当該信号中に含まれる情報をパケット化してフィルタ５０３に出力する（ステップＳ１０１～ステップＳ１０２）。

【０１０８】各パケットは、フラグ情報を有し、このフラグ情報にて当該パケットがマスターキーシードを含むパケットか、付加情報を含むパケットか、コンテンツ情報を含むパケットかを識別することができる。さらに、マスターキーシード、付加情報の最後のパケットには、終了フラグが記録されている。

【０１０９】フィルタ５０３は、マスターキーシード、付加情報それぞれのために、充分な大きさのバッファを有している。

【０１１０】入力されたパケットのフラグから、当該パケットにマスターキーシードが含まれていると判断した場合は、マスターキーシード用バッファに当該パケットを追加し、順次入力されるパケットのフラグに終了フラグが検出されたら、それまでにマスターキーシード用バッファに格納されたパケットをマスターキー生成部５０４に転送する（ステップＳ１０３～ステップＳ１０６）。

【０１１１】入力されたパケットのフラグから、当該パケットに付加情報が含まれていると判断した場合は、付加情報用バッファに当該パケットを追加し、順次入力されるパケットのフラグに終了フラグが検出されたら、それまでに付加情報用バッファに格納されたパケットを判定部５０７に転送する（ステップＳ１０７～ステップＳ１１０）。

【０１１２】入力されたパケットのフラグから、当該パケットにコンテンツ情報、チャネルサブキーＬが含まれていると判断した場合は、当該パケットをチャネルデコーダ５０９に転送する（ステップＳ１１１）。

【０１１３】マスタキー生成部５０４では、図１６のフローチャートに示すように、フィルタ５０３から転送されてきたパケットからマスターキーシードを抽出し、マスターキーを生成し、その生成されたマスターキーをマスターキー格納部５０５に格納する（ステップＳ１２１～ステップＳ１２３）。

【０１１４】判定部５０７では、図１７のフローチャートに示すように、フィルタ５０３からパケットが転送されてきたら、まず、マスターキー格納部５０５からマスターキーＫｍを読込み、当該パケットから抽出された付加情報をマスターキーＫｍを用いて復号する（ステップＳ１３１～ステップＳ１３３）。

【０１１５】付加情報には必ず端末ＩＤが含まれ、さらにチャネル番号とチャネルサブキーＨとが含まれている場合もある。

【０１１６】判定部５０７は、付加情報から端末ＩＤを抽出し、ＩＤ格納部５０６に予め格納されている自身の端末ＩＤとを比較し、一致していたときに限り、後続の処理を実行する。不一致のときは、処理を中止する（ステップＳ１３４）。

【０１１７】付加情報に含まれていた端末ＩＤと自身の端末ＩＤとが一致したとき、次に、付加情報にチャネルサブキーＨが含まれているか否かチェックし（ステップＳ１３５）、チャネルサブキーＨが含まれているときは、それをチャネルサブキー格納部５０８に格納する（ステップＳ１３６）。付加情報にチャネルサブキーＨが含まれていないときは、当該付加情報は、ＯＦＦ信号であると判断できるので、チャネルサブキー格納部５０８に既に格納されているチャネルサブキーＨを消去する（ステップＳ１３７）。

【０１１８】チャネルデコーダ５０９では、図１８のフローチャートに示すように、フィルタ５０３から転送されてきたパケットからチャネルサブキーＬを抽出したら（ステップＳ１４１～ステップＳ１４２）、チャネルサブキー格納部５０８からチャネルサブキーＨを読み出して（ステップＳ１４３）、チャネルキーＫｃｈを生成する（ステップＳ１４４）。ステップＳ１０９で、チャネルサブキー格納部５０８のチャネルサブキーＨが消去されている場合、処理を終了する。

【０１１９】チャネルサブキーＨとＬからチャネルキーＫｃｈを生成するアルゴリズムは、予めチャネルデコーダ５０９に格納されている。

【０１２０】さて、チャネルデコーダ５０９は、チャネルキーｋｃｈを生成すると、それを用いてフィルタ５０３から転送されてきたパケットから抽出される暗号化コ

ンテンツ情報を復号し（ステップＳ１４５）、復号されたコンテンツ情報を順次、Ｄ／Ａ変換部５１０に出力する（ステップＳ１４６）。

【０１２１】Ｄ／Ａ変換部５１０では、チャネルデコーダ５０９から送られてくるコンテンツ情報をアナログ信号に変換し（ステップＳ１４７）、再生部５１１にてアナログ信号の再生を行う（ステップＳ１４８）。

【０１２２】暗号の解読による不正な視聴を防止する観点から、暗号のキーは定期的に更新することが望ましい。例えば、放送に多重化して配信されるチャネルサブキーＬを変更することで、チャネルキーＫｃｈを容易に変更することができる。勿論、この場合、チャネルのコンテンツ情報は新しいチャネルキーＫｃｈによって復号可能である様に暗号化されていなければならない。なお、チャネルサブキーＬを放送波に多重化して配信しない場合もある。この場合、チャネルキーＫｃｈ＝チャネルサブキーＨとなる。

【０１２３】ところで、受信装置１００は、視聴許可の付加情報を受信すると、視聴禁止の付加情報を受信するまで、契約チャネルの番組視聴が可能である。ユーザがチャネルの番組視聴契約を解除したにも係わらず、視聴禁止の付加情報を受信しないケースも考えられる。例えば、受信装置の電源が一定期間切断された様な場合である。従って、視聴禁止の付加情報（ＯＦＦ信号）を解約後ある程度期間に渡って繰り返し放送する必要がある。

【０１２４】図１９は、新規契約に関する付加情報（ＯＮ信号）の送信量と、解約に関する付加情報（ＯＦＦ信号）の送信量の時間経過に伴う変動を示したものである。新規契約に関する付加情報（ＯＮ信号）の送信量と、解約に関する付加情報（ＯＦＦ信号）の送信量との和が、付加情報の総送信量である。新規契約に関する付加情報の送信は契約数に応じてバースト的な送信量となるのに対して、解約に関する付加情報の送信については、時間の経過とともに解約数を積分したような送信量の変化がみられる。

【０１２５】新規契約に関する付加情報の送信と、解約に関する付加情報の送信は、いずれもターゲットとする受信装置に確実に受信される保証を欠く。従って、何回か繰り返し放送されるが必要となる。

【０１２６】放送局側に設置される契約管理装置がＯＮ信号、ＯＦＦ信号となるような付加情報を配信することにより、前述したように、新規契約時と解約時にのみ付加情報を数回繰り返して配信すればよく、契約更新毎に（例えば毎月）全ての加入端末分の契約データを送信する方式に比較して、契約管理情報の送信量を大幅に減少させることが可能である。従って、チャネルのコンテンツ情報の送信量を増やすことができる。

【０１２７】（２）受信装置１００にて、受信した放送波から、何らかの方法で多重化した付加情報を剥ぎ取ってしまうと、視聴を禁止する付加情報（ＯＦＦ信号）の受信を回避して、不正に視聴が行われてしまうとこともあろう。そこで、このような不正行為に対処するため、放送局に設置されている契約管理装置は、一定数のバケット毎に、必ず付加情報を多重化して送信することとする。

【０１２８】送信すべき付加情報がない場合には、ダミーの付加情報を送信しても良い。この場合、受信装置１００のフィルタ５０３は、バケット数を数えるカウンタ（バケットカウンタ）を具備し、付加情報が到着するとカウンタをリセットする。カウンタの値が、予め定められた数値（Ｎ）よりも大となると、異常な状態と判断し、フィルタリング動作を停止するなど、処理中止動作を行う。

【０１２９】図２０に示すフローチャートは、受信装置１００のフィルタ５０３が、上記付加情報の受信状況を監視する処理を伴う場合の処理動作の一例を示したものである。なお、図２０において、変数ｃｏｕｎｔがバケットカウンタである。

【０１３０】まず、フィルタ５０３は、バケットカウンタを初期化する。すなわち、変数ｃｏｕｎｔを「０」に設定する（ステップＳ１５１）。フィルタ５０３は、Ａ／Ｄ変換部５０２から順次入力されるバケットに含まれるフラグ情報をチェックする（ステップＳ１５２）。

【０１３１】入力されたバケットのフラグから、当該バケットに付加情報が含まれていると判断した場合は（ステップＳ１５３）、バケットカウンタの値を「０」にリセットし（ステップＳ１５４）、付加情報用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでに付加情報用バッファに格納されたバケットを判定部５０７に転送する（ステップＳ１５５～ステップＳ１５７）。

【０１３２】入力されたバケットのフラグから、当該バケットに付加情報が含まれていないと判断したときは（ステップＳ１５３）、バケットカウンタの値を１つインクリメントする（ステップＳ１５８）。そして、バケットカウンタの値が予め定められたバケット数Ｎより大となったときは、異常なバケットの受信状態であると判断し、フィルタリング動作を停止するなど、処理中止動作を行う（ステップＳ１６０）。

【０１３３】一方、ステップＳ１５９で、バケットカウンタの値が予め定められた値Ｎより小さいときは、後続の処理を実行する。

【０１３４】すなわち、入力されたバケットのフラグから、当該バケットにマスターキーシードが含まれていると判断した場合は（ステップＳ１６１）、マスターキーシード用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでにマスターキーシード用バッファに格納されたバケットをマスターキー生成部５０４に転送する（ステップＳ１６２～ステップＳ１６４）。

【０１３５】また、入力されたバケットのフラグから、当該バケットにコンテンツ情報、チャネルサブキーＬが含まれていると判断した場合は、当該バケットをチャネルデコーダ５０９に転送する（ステップＳ１６５）。

【０１３６】放送局は定期的に（或いは適宜）チャネルサブキーＨ又はマスターキーを変更する。チャネルサブキーＨは、チャネルのコンテンツ情報を暗号化するキー（の構成要素）であるから、チャネルサブキーＨを変更した場合、チャネルのコンテンツ情報の暗号化も変更を受ける。受信契約を継続する受信装置に対しては、当該端末ＩＤとチャネル番号、当該チャネルのサブキーＨを含む付加情報を作成し、放送配信する。

【０１３７】マスターキーの変更は、契約管理よりも寧ろセキュリティの観点から行われる。マスターキーの変更はマスターキーシードの放送配信による。マスターキーを変更する際は、チャネルサブキーＨも同時に変更することが望ましい。

【０１３８】（３）図１４に示す受信装置１００にて受信される放送波には、次のような情報が含まれているものとする。

・　マスターキー・シード
・　［端末付加情報］Ｋｍ
・　［チャネル付加情報］Ｋｍ
・　［コンテンツ］Ｋｃｈ

端末付加情報は、各契約ユーザに固有の付加情報で、少なくとも次の情報を含んでいる。

・　端末ＩＤ
・　チャネル番号
・　有効／無効情報

なお、契約チャネルが１つのみの場合、チャネル番号は含まなくてもよい。

【０１３９】チャネル付加情報は、ユーザ少なくとも次の情報を含んでいる：

・　チャネル番号
・　チャネルキー

なお、チャネル付加情報には、さらにチャネルキーを識別するためのチャネルキーＩＤが含まれていてもよい。

【０１４０】図１４の受信装置の処理動作を図２１～図２３に示すフローチャートを参照して説明する。

【０１４１】まず、図２１において、受信部５０１が放送波を受信すると、Ａ／Ｄ変換部５０２がディジタル信号に変換するとともに、当該信号中に含まれる情報をバケット化してフィルタ５０３に出力する（ステップＳ１０１～ステップＳ１０２）。

【０１４２】各バケットは、フラグ情報を有し、このフラグ情報にて当該バケットがマスターキーシードを含むバケットか、端末付加情報あるいはチャネル付加情報を含むバケットか、コンテンツ情報を含むバケットかを識別することができる。さらに、マスターキーシード、端末付加情報、チャネル付加情報の最後のバケットには、終了フラグが記録されている。

【０１４３】フィルタ５０３は、マスターキーシード、端末付加情報、チャネル付加情報それぞれのために、充分な大きさのバッファを有している。

【０１４４】入力されたバケットのフラグから、当該バケットにマスターキーシードが含まれていると判断した場合は、マスターキーシード用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでにマスターキーシード用バッファに格納されたバケットをマスターキー生成部５０４に転送する（ステップＳ１０３～ステップＳ１０６）。

【０１４５】入力されたバケットのフラグから、当該バケットに端末付加情報が含まれていると判断した場合は、端末付加情報用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでに端末付加情報用バッファに格納されたバケットを判定部５０７に転送する（ステップＳ１７１～ステップＳ１７４）。

【０１４６】入力されたバケットのフラグから、当該バケットにチャネル付加情報が含まれていると判断した場合は、チャネル付加情報用バッファに当該バケットを追加し、順次入力されるバケットのフラグに終了フラグが検出されたら、それまでにチャネル付加情報用バッファに格納されたバケットを判定部５０７に転送する（ステップＳ１７５～ステップＳ１７８）。

【０１４７】入力されたバケットのフラグから、当該バケットにコンテンツ情報、チャネルサブキーＬが含まれていると判断した場合は、当該バケットをチャネルデコーダ５０９に転送する（ステップＳ１１１）。

【０１４８】マスタキー生成部５０４では、図１６のフローチャートと同様である。

【０１４９】判定部５０７では、図２２のフローチャートに示すように、フィルタ５０３からバケットが転送されてきたら、まず、マスターキー格納部５０５からマスターキーＫｍを読込み、当該バケットから抽出された付加情報をマスターキーＫｍを用いて復号する（ステップＳ１８１～ステップＳ１８３）。

【０１５０】入力されたバケットのフラグから、当該バケットに端末付加情報が含まれていると判断した場合は、端末付加情報から端末ＩＤを抽出し、ＩＤ格納部５０６に予め格納されている自身の端末ＩＤとを比較し、一致していたときに限り、後続のステップＳ１８６以降の処理を実行する。不一致のときは、処理を中止する（ステップＳ１８５）。

【０１５１】ステップＳ１８６では、端末付加情報からチャネル番号とそれに対応する有効／無効情報を抽出し、チャネル番号に対し「有効」が付随していたときは、ステップＳ１８７に進み、当該チャネル番号のコンテンツ情報の復号／再生が可能なように制御する。その

ために、例えば、各チャネル毎のオン／オフ制御を行うための配列情報をもち、有効の場合には、該当するチャネルの値を「１」とするようにしてもよい。また、チャネル番号に対し「無効」が付随していたときは、ステップＳ１８８に進み、当該チャネル番号のコンテンツ情報の復号／再生が不可能なように制御する。例えば、上記配列の該当するチャネルの値を「０」に設定する。

【０１５２】入力されたバケットのフラグから、当該バケットにチャネル付加情報が含まれていると判断した場合は、そのチャネル付加情報からチャネルキーＩＤとチャネルキーを取り出し、当該チャネル番号に対応させてチャネルサブキー格納部５０８に格納する。

【０１５３】チャネルデコーダ５０９では、図２３のフローチャートに示すように、フィルタ５０３にから転送されてきたバケットからコンテンツ情報を抽出して、先に取得されたチャネルキーを用いて復号し、Ｄ／Ａ変換部５０２に出力する（ステップＳ１９１～ステップＳ１９４）。

【０１５４】Ｄ／Ａ変換部５１０では、チャネルデコーダ５０９から送られてくるコンテンツ情報をアナログ信号に変換し（ステップＳ１９５）、再生部５１１にてアナログ信号の再生を行う（ステップＳ１９６）。

【０１５５】以上説明したように、チャネル付加情報は全ての受信装置に共通であり、端末付加情報は、チャネル（サブ）キーを含む場合に比べ短くなるため、付加情報としての契約制御情報を配信するに必要な放送帯域を節約することが可能となる。

（第２の実施形態）

１）放送システムの概略

契約受信装置に付加情報を放送配信する以外に、図２４に示すような配布形態も考えられる。

【０１５６】図２４は、本発明の契約管理装置および放送受信装置を用いた第２の実施形態に係る放送システムの概略構成を示したもので、放送局２００から衛星を利用して受信契約を行った各ユーザにコンテンツを提供するサービス形態の場合を示している。

【０１５７】図２４では、契約管理のための付加情報を各契約ユーザに放送配信するのではなく、例えば磁気カード等の携帯可能なカード型の記録媒体（以下、簡単にカードと呼ぶ）Ｐに記録しておき、それを当該受信装置に宅配又は郵送する点が、前述の第１の実施形態の場合と異なる。契約ユーザは、受信装置１００に受け取ったカードＰに記録された情報を読み取らせることにより、契約チャネルの受信が可能となる。

【０１５８】２）契約管理装置

図２５は、第２の実施形態に係る契約管理装置の構成例を示したもので、図３と同一部分は同一符号を付し、異なる部分について説明する。すなわち、図３の放送装置１３が図２５では、カード作成装置１５に置き換えられ、付加情報を地上波あるいは衛星放送を介して配信するのではなく、磁気カード、ＩＣカード等のカード型記録媒体（カード）に記録して、契約ユーザに配布するようになっている。

【０１５９】付加情報生成制御部９からの指示が「１９９７年１２月１日から４ヶ月間契約している契約ユーザの付加情報を送れ」であった場合、前述の図３に示した構成の契約管理装置では、付加情報を１ヶ月毎に作成しなくてはならないために１ヶ月毎に有効なチャネルキーと有効なマスターキーを検索して、図８のフローチャートに示す処理を行う必要がある。図２５に示す契約契約管理では、付加情報を放送によらずに例えば磁気カードに４ヶ月分の契約チャネルのチャネルキーに対応する付加情報を書込み、当該ユーザに配送すればよい。これにより、１ヶ月毎の配信、配布を行わなくてもよく、放送局側にもユーザ側にも煩雑を避ける意味で有利である。

【０１６０】２）受信装置

図２６は、第２の実施形態に係る受信装置１００の構成例を示したもので、前述の図２５に示したような放送局側に設置されている契約管理装置で作成されたカードから付加情報の読み取り、図１０に示したようなコンテンツ情報の配信装置から出力される放送波を受信するためのものである。なお、図１４と同一部分には同一符号を付している。

【０１６１】ここで、図２６に示す受信装置１００にて受信される放送波には、次のような情報が含まれているものとする。

・　マスターキーシード
・　チャネルサブキーＬ
・　チャネルサブキーＩＤ
・　［コンテンツ］Ｋｃｈ

チャネルサブキーＩＤは、付加情報の中のチャネルサブキーを識別するためのＩＤで、チャネルサブキーの変更が必ずマスターキーの変更を伴う場合には不要である。

【０１６２】カードＰには、マスターキーにて暗号化された付加情報が記録されている。

【０１６３】付加情報は、次のような情報が含まれているものとする。

・　端末ＩＤ
・　チャネル番号（複数も可）
・　チャネルサブキーＩＤ
・　チャネルサブキーＨ

なお、付加情報には、さらに、判定部５０７にてマスターキーによる復号が正しく行われたか否かを判定するための認証コード（例えば、予め定められた適当なビット列でもよい）が含まれていてもよい。

【０１６４】カードＰに記録されている付加情報は１つとは限らない。契約期間がマスターキーやチャネルサブキーＨの更新時期にまたがる場合、チャネルサブキーＨと暗号化のキーの異なる付加情報が複数記録されていてもよい。

【０１６５】図２７は、カードＰに記録される付加情報の例を示したもので、図２７（ａ）では、マスターキーＫｍとチャネルサブキーＨの更新時期が同じ場合（例えば、１ヶ月毎）、図２７（ｂ）は、マスターキーＫｍの更新時期が例えば２ヶ月毎であるのに対し、チャネルサブキーＨの更新時期が１ヶ月毎である場合に、それぞれユーザが２チャネル（チャネル番号Ｘ、Ｙ）を３ヶ月視聴する契約を行ったときにカードＰに記録される付加情報を示している。

【０１６６】図２７（ａ）に示すように、マスターキーＫｍとチャネルサブキーＨの更新時期が同じ場合、各月毎のチャネル毎のチャネルサブキーＨを各月毎のマスターキーＫｍで暗号化した３つの付加情報が記録されている。この場合、各チャネル毎のチャネルサブキーは１つのみなので、チャネルサブキーＩＤは必ずしも必要ない。

【０１６７】図２７（ｂ）に示すように、マスターキーＫｍとチャネルサブキーＨの更新時期が異なる場合、１つのマスターキーで暗号化されて生成される付加情報には、契約期間に応じて、各チャネル毎に複数（例えば２ヶ月分）のチャネルサブキーが記録されている場合もある。その場合、各チャネルサブキーはチャネルサブキーＩＤにてそれぞれ識別されている。

【０１６８】なお、図２７（ａ）、（ｂ）のいずれにおいても１つのマスターキーで暗号化される情報単位には認証コードが含まれていてもよい。

【０１６９】次に、図２６の受信装置の処理動作を図２８～図３０に示すフローチャートを参照して説明する。ここでは、カードＰに記録されている付加情報が例えば図２７（ｂ）に示すような場合を例にとり説明する。

【０１７０】まず、図２８に示すように、放送局側から配送されたカードＰをユーザがカードリーダ５１３に挿入する。カードリード５１３は、挿入されたカードＰから付加情報を読み取り、付加情報格納部５１２に格納する（ステップＳ２０１）。

【０１７１】図２９の説明に移り、受信部５０１が放送波を受信すると、Ａ／Ｄ変換部５０２がディジタル信号に変換するとともに、当該信号中に含まれる情報をバケット化してフィルタ５０３に出力する（ステップＳ１０１～ステップＳ１０２）。

【０１７２】各バケットは、フラグ情報を有し、このフラグ情報にて当該バケットがマスターキーシードを含むバケットか、チャネルサブキーＩＤを含むバケットか、コンテンツ情報を含むバケットかを識別することができる。さらに、マスターキーシードの最後のバケットには、終了フラグが記録されている。

【０１７３】フィルタ５０３は、マスターキーシード、付加情報のそれぞれのために、充分な大きさのバッファを有している。

【０１７４】入力されたバケットのフラグから、当該バケットにマスターキーシードが含まれていると判断した場合は、当該バケットを判定部５０７へ出力する（ステップＳ２１１～ステップＳ２１３）。

【０１７５】入力されたバケットのフラグから、上記以外のバケット、すなわち、当該バケットにコンテンツ情報、チャネルサブキーＬが含まれていると判断した場合は、当該バケットをチャネルデコーダ５０９に転送する（ステップＳ２１３）。

【０１７６】マスタキー生成部５０４の処理は、図１６のフローチャートと同様である。

【０１７７】次に、判定部５０７では、図３０のフローチャートに示すような処理を実行する。カードＰに記録されている付加情報は１つとは限らない。そこで、変数ｉをカードＰに記録されている複数の付加情報のインデックスに用い、付加情報中に含まれる、マスターキーによる復号が正しく行われた否かを判定するための認証コードのチェックをもって、有効な付加情報とみなすことにする。

【０１７８】まず、変数ｉの値を「０」にセットしてから（ステップＳ２２１）、付加情報格納部５１２に格納されている付加情報を１つづつ読み出す（ステップＳ２２２）。そして、マスターキー格納部５０５に格納されているマスターキーを読み出して（ステップＳ２２４）、付加情報を復号する（ステップＳ２２５）。復号された付加情報中に認証コードが含まれている場合は、その認証コードが正しいものであるか否かを確認する（ステップＳ２２６）。

【０１７９】認証コードが正しいものであるときは、契約期間内の正当なマスターキーで復号された有効な付加情報であると判断できる。従って、その付加情報に基づきステップＳ２２８以降の判定処理を実行する。一方、認証コードが誤ったものであるときは、変数ｉを１つインクリメントして（ステップＳ２２７）、付加情報格納部５１２に格納されている次の付加情報を読み出し、上記ステップＳ２２２～ステップＳ２２６を繰り返す。

【０１８０】ステップＳ２２８では、付加情報から端末ＩＤを抽出し、ＩＤ格納部５０６に予め格納されている自身の端末ＩＤとを比較し、一致していたときに限り、後続の処理を実行する。不一致のときは、処理を中止する。

【０１８１】次に、フィルタ５０３から転送されてきたバケットからチャネル番号毎のチャネルサブキーＩＤを抽出し、さらに、付加情報からチャネル番号毎のチャネルサブキーＩＤを１つづつ取り出し、それを比較する（ステップＳ２２９）。一致していたら、付加情報から当該チャネルサブキーＩＤに対応するチャネルサブキーＨを抽出し、チャネルサブキー格納部５０８へ格納する（ステップＳ２３１）。不一致のときは、付加情報から当該チャネル番号の次のチャネルサブキーＩＤを取り出して（ステップＳ２３０）、再び、先にバケットから抽

出されたチャネルサブキーＩＤと比較すればよい。

【０１８２】チャネルデコーダ５０９、Ｄ／Ａ変換部５１０、再生部５１１の処理動作は、図１８のフローチャートと同様である。

【０１８３】（用語の説明）以下の実施形態について述べる前に用語の定義を行なう。限定受信を行なうためチャネル毎の契約状態を記述した情報を契約情報と呼ぶ。例えば各チャネルにチャネル番号を付け、チャネル番号に対応したビットが「１」であるか否かによりチャネルの契約状態を表すことができる。これを特にチャネル契約情報という。

【０１８４】契約情報には、これ以外にも様々な形態があり得る。例えば、図１１（ｂ）のチャネルサブキーＨとチャネル番号の組も当該チャネル番号のチャネルが契約されていることを示す契約情報であり、図１２のチャネル番号と有効／無効の情報の組も当該チャネル番号の契約状態を示す契約情報である。

【０１８５】契約情報は受信装置ＩＤと相互にリンクされており、受信装置ＩＤは、当該契約情報が適応される受信装置の識別子を示している。この意味で契約情報と受信装置ＩＤは一体のものであり、受信装置ＩＤと契約情報の組を単に契約情報と呼ぶこともある。今後両者を区別する必要がある時には、前者を狭義の契約情報、後者を広義の契約情報として区別する。

【０１８６】また、以下の実施形態では、契約情報（契約情報と受信装置ＩＤの組）は（改竄を防いだり、不利な契約情報の取得を防ぐ目的で）暗号化されて放送配信もしくは磁気カード等の記録媒体に記載され郵送等で送られるが、ここで契約情報と一緒に暗号化されるデータセットをまとめて受信契約情報と呼ぶことにする。受信契約情報には、契約情報も含まれる。更に受信契約情報にデータの識別子など本システムに必要な情報を付加したものを契約情報バケットという。

【０１８７】実施形態は、チャネルキーと契約情報の分離の程度によって分類されている。即ち、受信契約情報にチャネルキーをどの程度含めるかによって区別される。

【０１８８】前述の第１の実施形態は、受信契約情報の中にチャネルキーの一部が含まれることを特徴とする請求項４に記載の放送受信装置に対応する実施の形態である。

【０１８９】前述の第２の実施形態は、受信契約情報の中にチャネルキーを１ビットも含まないことを特徴とする請求項２に記載の放送受信装置に対応する実施の形態である。

【０１９０】第３の実施形態は、受信契約情報の中に暗号化されたチャネルキーを復号するためのチャネルキー復号鍵が含まれることを特徴とする請求項３に記載の放送受信装置に対応する実施の形態である。

【０１９１】第４の実施形態は、受信契約情報の中にチャネルキーそのものを含めることを特徴とする請求項５に記載の放送受信装置に対応する実施の形態である。

【０１９２】第５の実施形態は、課金制御部（課金チップ）の製造上必要なテスト用スキャンパスラッチ部の構成を示したもので、第１～４の実施形態に共通に利用できる技術である。

【０１９３】なお、第３の実施形態以降の説明において、放送受信装置内部で限定受信の仕組みを実現する構成部を課金制御部と呼ぶ。なお、課金制御部はハードウェアにて構成され、しかもＬＳＩ化されているものが望ましい。このようなＬＳＩ化された課金制御部を課金チップと呼ぶのもよい。いずれにしても、課金制御部には限定受信のための秘密情報が含まれているので内部のメモリやハード構成に関して外部から容易に読み出し、書き込み、変更ができない耐タンパ構造を仮定している。

【０１９４】また、課金制御部内部のメモリには全ての放送受信装置に共通のマスター鍵が書き込まれており、主に受信契約情報を復号するのに用いられる。また、受信装置ＩＤは、放送受信装置毎個別に設定され、課金制御部内部の不揮発性メモリの中に記録されている。

【０１９５】第１の実施形態と第２の実施形態においては上記の用語が次のような形で述べられている。すなわち、受信契約情報を付加情報、課金制御部を復号ユニット、受信装置ＩＤを端末ＩＤ。

【０１９６】また、第１の実施形態と第２の実施形態で述べられているチャネル番号、フラグ情報は、それぞれ、第３の実施形態と第４の実施形態で述べられているチャネル識別子、情報識別子にあたる。

【０１９７】（第３の実施形態）

１）放送受信装置

図３１は、本実施形態に係る放送受信装置の構成を概略的に示したものである。

【０１９８】本実施形態の放送コンテンツは図３２に示すように４段の暗号化機構によって保護されている。チャネルキーＫｃｈは、スクランブルされた放送コンテンツを復号するための鍵であり、一般にチャネル毎に異なり、短期間で変更される。

【０１９９】図３３に示すように放送波には２種類の情報（放送コンテンツ情報、チャネルキー情報）が含まれている。ここで放送コンテンツのデスクランブルはチャネルキー情報から得られたチャネルキーＫｃｈで行なわれる。

【０２００】さて、図３２の説明に戻り、チャネルキー情報に含まれるチャネルキーＫｃｈは暗号化されており、チャネルキー復号鍵K_Hで復号できる。このチャネルキー復号鍵K_Hはチャネルに依存しない、システム共通のもので、暗号化された受信 契約情報に含まれている。

【０２０１】暗号化された受信契約情報は、予め全ての放送受信装置に共通に存在するマスター鍵K_Mで復号さ

れる。更にマスター鍵K_Mは、マスター鍵シードS_Mによって 定期的に変更される。

【０２０２】スクランブル放送波をデスクランブルするためには、チャネルキーＫｃｈを取得しなくてはならず、取得のためには暗号化されたチャネルキーを復号する必要があり、その復号鍵K_Hは、暗号化された受信契約情報に含まれている。暗号化された受信契約情報は、マスター鍵K_Mで復号される。また、マスター鍵で復号された受信契約情報の中には、受信装置ＩＤに対応付けられた各受信装置宛の狭義の契約情報も一緒に含まれており、放送受信装置はこれを自分のものであると判断した上で取得し、契約情報格納部にこれを格納する。

【０２０３】放送受信時には、契約情報格納部から契約情報を参照し、当該チャネルが契約済であった場合のみ前記の手段で取得したチャネルキーＫｃｈをデスクランブル部に送り、放送波をデスクランブルする。

【０２０４】このようなシステムを取ることにより、チャネルキーＫｃｈを取得するためにチャネルキー復号鍵K_Hを取得しなければならず、更に契約情報とチャネルキー復号鍵K_Hが受信契約情報の暗号化により不可分になるので、チャネルキー復号 鍵K_Hを取得するためには、契約情報を取得しなければならなくなり、契約を確実に遵守させることが可能となる。

【０２０５】以下では更に詳しく説明する。本実施形態の放送受信装置で受信されるチャネルには、通常チャネルと契約情報チャネルがあり、通常チャネルには通常の放送コンテンツが流れている。その構造は、図３３に示す通りである。ここで、放送コンテンツ情報は、図３４に示すように、暗号化された放送コンテンツ（Ｃ）とチャネルキー識別子（ＫＩＤ）とチャネル識別子（ＣＩＤ）と情報識別子（ＩＩＤ）とに分かれる。

【０２０６】ここで、情報識別子とは当該情報が放送コンテンツ情報であることを示すもので、例えば、「０００１」であってもよい。また、チャネル識別子は、当該放送コンテンツがどのチャネルのコンテンツであるかを識別するための情報である。更に、チャンネルキー識別子は、当該暗号化コンテンツを復号することができるチャネルキーを識別するための情報である。この利用法及び構造は後で詳しく述べる。

【０２０７】一方、チャネルキー情報は、図３５に示すように、暗号化されたチャネルキーとチャネルキー識別子、チャネル識別子、チャネルキー復号鍵識別子及び情報識別子からなっている。

【０２０８】ここでチャネルキー識別子は当該チャネルキーを識別するための情報で暗号化コンテンツを復号する際に利用される。チャネル識別子は当該チャネルキーで復号できるコンテンツ情報のチャネルを示す情報である。チャネルキー復号鍵識別子は暗号化されたチャネルキーの復号鍵を識別するために用いられる。この利用法及び構造は後で詳しく述べる。情報識別子は当該情報がチャネルキー情報であることを示すもので、放送コンテンツ情報等の他の情報と区別するために、例えば「０００２」であってもよい。

【０２０９】契約情報チャネルの構造は図３６に示す通りで、契約情報バケットとマスター鍵シードからなる。

【０２１０】ここで、契約情報バケットは図３７に示すように、暗号化された受信契約情報、チャネルキー復号鍵識別子、マスター鍵識別子、情報識別子からなっている。

【０２１１】チャネルキー復号鍵識別子は、当該受信契約情報に含まれるチャネルキー復号鍵を識別する情報で、暗号化されたチャネルキーを復号する際の復号鍵の識別に用いられる。マスター鍵識別子は当該契約情報バケットに含まれる暗号化受信契約情報が復号できるマスター鍵を識別するために用いられる。情報識別子は当該情報が契約情報バケットであることを示すもので、例えば「０００３」であってもよい。

【０２１２】受信契約情報は、図３８に示すように、受信装置ＩＤ、チャネル契約情報、チャネルキー復号鍵K_Hからなっている。受信装置ＩＤは当該受信装置に固有の識別子（ＩＤ）であり、当該契約情報が当該受信装置宛のものであるか否かの判定に用いる。チャネル契約情報はユーザに提供可能な複数のチャネルのそれぞれに１ビットづつ割り当て、当該ユーザが契約しているチャネルに該当するビットは「１」、そうでないビットには「０」を割り当てることにより、当該受信装置の契約状態を表す。チャネルキー復号鍵K_Hは、チャネルキーＫｃｈを復号するた めの鍵である。

【０２１３】マスター鍵シード情報は、図３９に示すように、マスター鍵シードとマスター鍵識別子、情報識別子からなっている。マスター鍵シードはマスター鍵を生成するためのシード情報である。マスター鍵識別子は当該マスター鍵シードで生成されたマスター鍵の識別情報である。情報識別子は当該情報がマスター鍵シード情報であることを示すためのものであり、例えば「０００４」としても良い。

【０２１４】ここでチャネルキー識別子の役割について述べる。

【０２１５】放送コンテンツ情報は、図３４に示すように、チャネルキーによって暗号化された放送コンテンツ情報Ｃとチャネルキー識別子ＫＩＤとチャネル識別子ＣＩＤと情報識別子ＩＩＤよりなる。チャネルキー識別子ＫＩＤは、暗号化された放送コンテンツ情報Ｃがどのチャネルキーで暗号化したものかを示すもので、チャネルキーに固有に付けられた識別子（ＩＤ）である。この場合、スクランブル放送コンテンツを復号するチャネルキーは一意に決まるのでシステム的に明解である。

【０２１６】しかし、実装上は当該チャネルキーを何時の時点まで保持しなくてはならないかが明確でないばかりか、ＩＤを一意的にするためＩＤの長さが長くなり、

大きな記憶容量を要するなどの問題がある。そこで、ここでは１ビットの相対ＩＤを付ける例を考える。即ち、（暗号化して）送信するチャネルキーに対して（交互に）「０」もしくは「１」という１ビットのＩＤを付け、新しいチャネルキーを受信したら、（図４１に示すような）メモリ上のチャネルキーを更新して行く。

【０２１７】この際、（当然のことながら）新しいチャネルキーはそれに対応するスクランブル放送波の送信に先立って送られなくてはならない。このため送信のスケジュールは、全ての放送受信装置で鍵の復号とメモリへの格納が完了する時間を考え、図４０のようにチャネルキー切替え時点でチャネルキー「０」とチャネルキー「１」の送信がオーバーラップする時間帯（Ｔｘ１、Ｔｘ２）が存在する。この時間帯をどれだけ取るかは放送受信装置が暗号化チャネルキーを復号して、メモリに格納する時間をどれだけに見積もるかによっている。このようにすることにより、チャネルキーのＩＤに相対ＩＤを用いることができる。

【０２１８】鍵の相対ＩＤの概念は本実施形態における他の全ての鍵（チャネルキー復号鍵、マスター鍵）にも同様の方式で用ることができる。

【０２１９】次に、図３１に示した放送受信装置の構成と、その処理動作について、図４２～図４５に示すフローチャートを参照して説明する。

【０２２０】放送波は、チャンネルに関わらず受信部１１０１で受信される（図４２のステップＳ１００１）。受信された放送波はＡ／Ｄ変換部１１０２でＡ／Ｄ変換され（ステップＳ１００２）、誤り検出／訂正部１１０３で誤り訂正符号などを用いることにより、伝送途中で載ったノイズ等の除去を行なう（ステップＳ１００３、ステップＳ１００４）。

【０２２１】ノイズが除去された放送波は、チャネル選択部１１０４に送られ、例えば、通常のテレビ受信機と同様なチャネルを選択するためのチャネル選択インターフェース（Ｉ／Ｆ）１１０５などを用いて選択されたチャネルに対応した放送波と契約情報チャネルの放送波を課金制御部１１０６に送る。

【０２２２】課金制御部１１０６では、これをフィルター部１１０７に送り、放送コンテンツ情報とチャネルキー情報と契約情報パケット及びマスター鍵シード情報に分離する。この分離は各々の情報識別子によって行なう。

【０２２３】さて、受信した情報がマスター鍵シード情報であれば（ステップＳ１０１３）、これはフィルター部１１０７から分離され、マスター鍵生成部１１１１に入力される（ステップＳ１０１４）。マスター鍵生成部１１１１ではマスター鍵シード情報からマスター鍵シードとマスター鍵識別子を分離し、マスター鍵シードから乱数生成や暗号化のアルゴリズムを用いてマスター鍵を生成し（ステップＳ１０１５）、マスター鍵識別子（例えば、相対ＩＤで「０」または「１」）に示されたメモリに格納する（ステップＳ１０１６）。

【０２２４】ここで生成アルゴリズム及び乱数生成のための秘密情報は全ての放送受信装置及び放送局に共通であり、課金制御部１１０６内の不揮発性メモリか外部からアクセスできないＲＯＭに秘匿されている。このため暗号化されていないシードを送っても１つのマスター鍵を共有することができるのである。

【０２２５】受信した情報が契約情報パケットであれば（ステップＳ１０１１）、フィルター部１１０７から契約情報復号部１１１０へ送られる（ステップＳ１０１２）。契約情報復号部１１１０では、契約情報パケットに含まれているマスター鍵識別子に対応するマスター鍵をマスター鍵格納部１１１２から取得する（ステップＳ１０４１）。この時マスター鍵格納部１１１２に対応するマスター鍵が存在しない場合は、その時点で処理を終了する。ここで「ＮＵＬＬ」（全てのビットが「０」）のマスター鍵は存在しないと仮定し、「ＮＵＬＬ」が取得された場合にマスター鍵が格納されていないと判断しても良い。

【０２２６】マスター鍵が出力された場合（ステップＳ１０４２）、契約情報パケット内にある暗号化された受信契約情報を当該マスター鍵で復号する（ステップＳ１０４３）。復号された受信契約情報の中から受信装置ＩＤを取得し、認証部１１１４は、それを受信装置ＩＤ格納部１１１３に格納されている受信装置ＩＤと比較する（ステップＳ１０４４）。もし、一致したら（ステップＳ１０４５）、当該受信装置ＩＤとリンクされたチャネル契約情報をチャネル契約情報格納部１１１６に格納する（ステップＳ１０４６）。一致した場合でもしない場合でも、チャネルキー復号鍵K_Hは当該契約情報パケットに含まれるチャネルキー復号鍵識別子（例えば、相対ＩＤで「０」または「１」）に示されたメモリに格納する（ステップＳ１０４７）。

【０２２７】受信した情報がチャネルキー情報であり（図４２のステップＳ１００８）、さらに、当該チャネルキー情報中のチャネル識別子をチェックして、チャネル選択Ｉ／Ｆ１１０５で選択されたチャネルのチャネルキー情報であるときは（ステップＳ１００９）、フィルター部１１０７からチャネルキー復号部１１０９へ送られる（ステップＳ１０１０）。

【０２２８】チャネルキー復号部１１０９では、チャネルキー情報に含まれるチャネルキー復号鍵識別子に対応するチャネルキー復号鍵をチャネルキー復号鍵格納部１１１５から取得する（図４４のステップＳ１０３１）。ここでもマスター鍵取得の時と同様に、「ＮＵＬＬ」のチャネルキー復号鍵が取得された時は、まだチャネルキー復号鍵が格納されていないと判断し、そこで処理を終える。「ＮＵＬＬ」でないチャネルキー復号鍵が取得された場合は（ステップＳ１０３２）、それを使ってチャ

ネルキー情報に含まれる暗号化チャネルキーを復号する（ステップＳ１０３３）。

【０２２９】復号されたチャネルキーはチャネルキー情報に含まれるチャネルキー識別子（例えば、相対ＩＤで「０」または「１」）に示されたメモリへ格納する（ステップＳ１０３４）。

【０２３０】受信した情報がスクランブル放送コンテンツ情報であり（図４２のステップＳ１００５）、さらに、当該放送コンテンツ情報中のチャネル識別子をチェックして、チャネル選択Ｉ／Ｆ１１０５で選択されたチャネルの放送コンテンツ情報であるときは（ステップＳ１００６）、フィルター部１１０７からデスクランブル部１１０８へ送られる（ステップＳ１００７）。

【０２３１】デスクランブル部１１０８では、チャネルキー出力部１１２０へチャネル識別子を送り、当該チャネルのチャネルキーを取得する（ステップＳ１０２１）。チャネルキー出力部１１２０は、契約判定部１１１８に当該チャネルが契約済みかどうかを問い合わせる。これを受けて契約判定部１１１８は、チャネル契約情報格納部１１１６のチャネル契約情報を参照して、当該チャネルが契約済みか判定し、契約済の場合「１」、未契約の場合「０」を出力する。チャネル契約情報は例えば、契約済みの場合「１」、未契約の場合「０」といったものでもよい。

【０２３２】契約判定部１１１８から「０」が出力された場合は、チャネルキー出力部１１２０は「ＮＵＬＬ」をデスクランブル部１１０８に出力して、契約されていないことを示す。契約判定部１１１８から「１」が出力された場合、チャネルキー出力部１１２０は、チャネルキー格納部１１１７からチャネルキー識別子に対応するチャネルキーを取得する。ここでもマスター鍵取得の時と同様に「ＮＵＬＬ」のチャネルキーが取得された時は、まだチャネルキーが格納されていないと判断し、そこで処理を終える。「ＮＵＬＬ」でないチャネルキー復号鍵が取得された場合は（ステップＳ１０２２）、デスクランブル部１１０８は、それを使ってスクランブル放送コンテンツを復号し、出力する（ステップＳ１０２３、ステップＳ１０２４）。

【０２３３】なお、受信装置ＩＤ格納部１１１３は、課金制御部１１０６内の耐タンパな不揮発性メモリで構成され、受信装置ＩＤが課金制御部１１０６外へ出力されることがないことが望ましい。そのような課金制御部１１０６であれば受信装置ＩＤを読み取ることは極めて困難なので契約情報を偽造することは事実上不可能とすることができる。また、マスター鍵についても同様の耐タンパ性を仮定すれば、課金制御部１１０６内のメモリから読み取って、送信されてくる契約情報バケットに含まれる受信契約情報を端から復号し、当該放送受信装置に不利な（当該受信装置の）受信契約情報を含む契約情報バケットのみをカットする攻撃も不可能となる。

【０２３４】また、課金制御部１１０６に対して十分な耐タンパ性を仮定すれば、マスター鍵は読み出されることはないので、マスター鍵シードを送ってマスター鍵を変更する必要もなくなる。この場合、マスター鍵は固定になるので本実施形態に関してマスター鍵シードを入力して、マスター鍵を変更する部分の構成を削ることができる。

【０２３５】さらに、マスター鍵を格納するマスター鍵格納部１１１２は、受信装置ＩＤ格納部１１１３と同様に、課金制御部１１０６内の耐タンパな不揮発性メモリで構成されていてもよいし、課金制御部１１０６内の回路として設定されていても良い。このようにすることにより、回路規模が削減できる。

【０２３６】しかし、ハードウェアの耐タンパ性は現在のところ完全なものは存在しない、即ち、耐タンパ性にはレベルがあり、ハードウェア内部のメモリや回路の内容の読み込み書き込みが、容易に手に入りしかも安価な装置を使って実現できるレベルのものから、本格的な装置を使って一定の技術を持った者が時間を掛けなければできないものまで様々である。従ってコストとの兼ね合いの観点から課金制御部１１０６に強い耐タンパ性を持つハードウェアを利用できない場合もある。このためあまり強い耐タンパ性を仮定せず、システム側で耐タンパ性を補強することは重要である。

【０２３７】耐タンパ性が崩壊した場合、課金制御部１１０６内に秘匿されているマスター鍵と受信装置ＩＤが読み取られる可能性がある。その場合、契約情報の偽造が可能である。これを防ぐため次のような工夫は重要である。

【０２３８】契約情報の偽造を防ぐには、公開鍵方式が有用である。公開鍵方式は例えば放送局側で秘密鍵を使って暗号化データを作り、課金制御部１１０６内にある公開鍵によってそのデータを処理することができる方式である。ここで、公開鍵から秘密鍵を算出することが計算量的に極めて困難で、事実上不可能なことから、秘密鍵を知らない者が公開鍵で復号して意味のあるデータを作成することができないところに特徴がある。即ち、契約者が自分に都合の良い暗号化された受信契約情報を作成しようと思っても、秘密鍵を知らないので極めて困難となるのである。この意味で受信契約情報の暗号化に公開鍵暗号を用いることは有用である。

【０２３９】さらに、受信契約情報に公開鍵暗号によるデジタル署名を含めるという構成も有用である。デジタル署名とは、受信契約情報からデジタル署名を除いた部分にハッシュ関数というある種の要約関数を施して要約した値（これをハッシュ値という）に対して秘密鍵を使って暗号化したものである。デジタル署名は前記同様秘密鍵を知らないと事実上作成できないばかりか、公開鍵によってデジタル署名を復号し得られたハッシュ値と、別途受信契約情報からデジタル署名を除いた部分に対す

るハッシュ値を比較することによりデジタル署名を検証することが可能である。

【０２４０】この場合、デジタル署名の検証は当該受信装置ＩＤが受信契約情報の中に存在した時のみに行なうことにすると良い。何故ならデジタル署名の検証には時間がかかり、基本的に契約情報を更新する必要がある場合以外、署名の検証を行う必要はない。

【０２４１】受信契約情報にデジタル署名を付けたときの放送受信装置の構成は、図３１における認証部１１１４を図６８に置き換えれば良い。その場合の受信契約情報の構成を図６９に示す。勿論、後述する図４９に示すように、データ圧縮も可能である。しかし、前記の手段を取っても次のような攻撃法は可能である。即ち、一旦全てのチャンネルに対して契約した契約者が、その時送信された契約情報バケットを記録しておく。ここで、契約者がマスター鍵と受信装置ＩＤを知っていれば当該放送受信装置の契約情報を特定することができるが、例えそれらを知らなくても契約情報放送波を記録しておき、視聴が可能になる前の一定期間に当該放送受信装置に対する契約情報を含む契約情報バケットが流れたと考えるの自然である。次に契約者は全チャンネルを解約し、そのため全チャンネルは視聴できなくなるが、視聴できなくなった時点で先に記録した古い暗号化受信契約情報を含む契約情報バケットを再び何らかの手段で課金制御部１１０６に入力して以前の（有利な）契約情報に置き替えてしまうことは原理的には可能である。しかも、この場合はデジタル署名も正しいので放送受信装置は契約情報を受理してしまう。このような攻撃を防ぐためには定期的にデジタル署名用の公開鍵を変更する必要がある。変更してしまえば古いデジタル署名は無効になる。変更の仕方は情報識別子を使うことにより情報を識別し、バケット内のデジタル署名用公開鍵を不揮発性メモリに格納すれば良い。この鍵は公開鍵であるため特に暗号化する必要はないが、機密保持のためマスター鍵で暗号化する構成も考えられる。

【０２４２】また、次々と送られてきて即時に復号化されなければならない放送コンテンツに関して、暗号化は共通鍵暗号が望ましい。これは共通鍵暗号が公開鍵暗号よりも、１００倍～１０００倍高速であるからである。チャネルキーの暗号化にも同様に共通鍵暗号が望ましい。チャネルキーは偽造したりしても意味のないものであるため、公開鍵暗号を採用する意味は殆どない。

【０２４３】更に、マスター鍵生成部１１１１の入力となるマスター鍵シードであるが、これは文字通り乱数のシードでも良いが、共通鍵暗号や公開鍵暗号を使って暗号化したマスター鍵であっても良い。その場合それらのための復号鍵が課金制御部１１０６内に耐タンパな不揮発性メモリもしくは回路として記録されていないといけない。

【０２４４】本実施形態のチャネルキー格納部１１１７、チャネルキー復号鍵格納部１１１５、マスター鍵格納部１１１２は、放送受信装置の電源オフ時に「ＮＵＬＬ」にクリアされなくてはならない。何故なら再び電源をオンする時には、これらの鍵は変更されている可能性が高いからである。ＮＵＬＬクリアされていれば、当該キーがまだ格納されていない場合は復号動作が起きないので、対応しない鍵で復号してしまって無意味なデータを出力する心配はない。

【０２４５】また、上記事項に関連して間違ったチャネルキー情報を課金制御部１１０６が受けとってしまった場合を考えよう。勿論誤り訂正符号を用いた誤り検出／訂正は、誤り検出／訂正部１１０３で行われるのであるが、それでも確実ではない。もし、誤った鍵情報（例えば、チャネルキーもしくはマスター鍵シード）のまま課金制御部１１０６が受け取ってしまえば、誤った鍵や契約情報を格納し、それを使って誤った復号や限定受信が行なわれる。一般に暗号は鍵が１ビットでも違えば復号結果は正しい結果とはかけ離れてしまう。これは、鍵から平文（元のデータ）が類推できないという安全性の要求からきたものであり、このような性質を持っていない暗号は弱い暗号なので利用できない。そこで暗号化した鍵情報や契約情報を含む重要な情報に認証子をつける方式が考えられる。

【０２４６】次に、図４６～図４８を参照して、暗号化された鍵情報や契約情報を含む重要な情報に認証子を用いた場合について説明する。暗号化した鍵情報に付ける認証子は、復号した結果得られる鍵情報から何らかのアルゴリズムで演繹されるものである。そのため復号した結果から認証子を求める演算を施して得られたものと認証子を比較して一致していれば誤りのないデータと考える訳である。ここで認証子は、例えば鍵ｋを鍵ｋで暗号化したものの上位３２ビットなどとしても良い。ここで鍵を６４ビットと仮定すれば、認証子は最大６４ビットとなる。当然だがこの方式では誤り検出しかできない。

【０２４７】また、誤りがあっても検出に失敗してしまう確率は認証子の長さによって決まり、認証子の長さを１とすると、１／２'である。これは認証子が長ければ長いほど失敗確率が減ることを意味している。即ち要求される失敗確率によって認証子の長さを決めれば良いことになる。その意味で要求される失敗確率が相当に低く、６４ビットの認証子では間に合わない場合もあるだろう。この場合は別系統の認証子を更に付ける必要がある。別系統の認証子とは基本的に別のアルゴリズムで作った認証子であるが、その実現が困難な場合は、現在のアルゴリズムを使って、鍵ｋをある一定の関数で変換した後、同じアルゴリズムで作成したものを認証子とする。もしくは最初に得られた認証子に対して更に同じアルゴリズムを掛けて認証子を生成することができる。認証子生成アルゴリズムに暗号アルゴリズムを使うと表面的なビット列として相互に関係がない認証子を作ること

ができる。これは、暗号アルゴリズム自体にランダム性があるからである。殆ど「０」に近い失敗確率を求められた場合はこのようにして十分多くの認証子を用意し、それを一定の手段で縮めたものを用いれば良い。

【０２４８】本実施形態において認証子付きの暗号化鍵情報を考える場合は、暗号化鍵情報の部分を図４６に置き換え、図３１におけるチャネルキー復号部１１０９、契約情報復号部１１１０（もしくは認証部１１１４）の内部にそれぞれ認証子確認部を設け、認証に失敗した場合は、鍵を出力しないように構成すれば良い。

【０２４９】受信契約情報やマスター鍵シードにも認証子を付ける必要があるが、ここでマスター鍵には公開鍵暗号系も考えられるので６４ビットのように区切れの良いブロックになっていない。公開鍵暗号系の鍵は共通鍵暗号系の鍵よりも長いので図４７に示すようにブロックに区切り、それぞれのブロックで上記の手段で認証子を作り、それらの認証子同士の排他的論理和（ＥｘＯＲ）をとるなどという手段で認証子を作ることが可能である。

【０２５０】また、受信契約情報に鍵情報（本実施形態の場合はチャネルキー復号鍵）が含まれる場合は、、その鍵情報を使って上記ブロック分割でできた各ブロックを暗号化し、上記同様にして排他的論理和（ＥｘＯＲ）を取って認証子を作ることができる。

【０２５１】また、図４８に示すように、第１ブロックの第１の認証子を前記の例と同じ手法で作り出して、第２ブロックと排他的論理和（ＥｘＯＲ）を取る。排他的論理和を取ったものに対して前記のアルゴリズムで第２の認証子を作る。これを繰り返すことによって最終的に認証子が生成される。いずれの場合も、６４ビットにブロック化するために、必要に応じて図４７に示したようなＰＡＤというＮＵＬＬデータ（疑似データ）を入れる。従って、マスター鍵シードに認証子を付ける場合もマスター鍵生成部１１１１の中に認証子を確認するプロセスを入れればその検証を実現できる。

【０２５２】最後に、受信契約情報の構成の拡張について触れておく。受信契約情報は、図３８に示すように、受信装置ＩＤ（ＴＩＤ）とチャネル契約情報（ＣＨＳ）とチャネルキー復号鍵から構成されている。

【０２５３】チャネルキー復号鍵は安全性確保のためにチャネルキーよりも鍵サイズを長くとっている。例えばＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などの標準的な暗号を用いるとチャネルキーは６４ビット、チャネルキー復号鍵は１２８ビットのように構成される。ここで、受信装置ＩＤ（ＴＩＤ）は放送受信装置をユニークに定めれば良いので高々５０ビット程度でよい。チャネル契約情報（ＣＨＳ）は、チャネル数だけのビットが必要だが例えば３０チャンネルあれば３０ビットで良い。従ってチャネルキー復号鍵以外の部分は８０ビットで半分以上はチャネルキー復号鍵が占める。

【０２５４】ところでチャネルキー復号鍵は全ての放送受信装置に共通であり、受信契約情報（少なくとも、受信装置ＩＤとチャネル契約情報を含む）の受信を確実にするために受信契約情報に入れてある。何故なら、自分に不利な受信契約情報でもチャネルキー復号鍵が含まれていれば受信せざるを得ないからである。この主旨からは１つの契約情報バケットに複数の放送受信装置に対する受信契約情報を入れても問題はなく、その方が送信データが少なくなるのである。

【０２５５】そこで、図４９に示すように、契約情報バケットを構成する。なお、図４９では、契約情報バケット中の受信契約情報に関する部分のみを示している。

【０２５６】ここではチャネルキー復号鍵の両側に対応する受信装置ＩＤ（ＴＩＤ）とチャネル契約情報（ＣＨＳ）の組を複数配置している。ここで契約情報バケットの先頭部分にチャネルキー復号鍵を配置しないのは、受信契約情報の暗号化にＤＥＳのような共通鍵暗号を使った場合、６４ビットを１ブロックとしてその単位で暗号化することが多いため、チャネルキー復号鍵が１２８ビットであった場合、最初の２ブロックがチャネルキー復号鍵である。もし、このことが分かると、受信機を改造して最初の２ブロックのみを復号し、チャネル契約情報を取得せずにチャネルキー復号鍵を取得することが可能になる。同様のことは、チャネルキー復号鍵を最後に配置した場合にも言える。ただし、６４ビット単位ではない公開鍵暗号のような暗号系で暗号化する場合はこの限りではない。また、いずれの場合も暗号化ブロックの切れ目がデータの切れ目と一致しないようにすることが望ましい。更に、データの無駄を省く為全体のサイズは受信契約情報を暗号化する暗号系におけるブロックサイズと一致させることが望ましい。

【０２５７】更に、受信契約情報を図５０に示すように拡張すると、より多くの契約情報が１つの契約情報バケットで送れることになる。なお、図５０では、契約情報バケット中の受信契約情報に関する部分のみを示している。

【０２５８】図５０に示す受信契約情報は、チャネル契約情報（ＣＨＳ）を１つしか含まないことを特徴としており、複数ある受信装置ＩＤ（ＴＩＤ）は全て、前記チャネル契約情報を契約内容とする放送受信装置の受信装置ＩＤである。即ち、図４９の受信契約情報では１つのチャネル契約情報と１つ受信装置ＩＤをリンクして記録しているところを、図５０では、１つのチャネル契約情報に複数の受信装置ＩＤをリンクして記録していることが特徴で、これにより契約情報バケットで送れる受信契約情報の量が更に多くなる。

【０２５９】しかし、問題点もある。例えば、チャネル契約情報の種類が多くて、対応する契約者が少ないような場合は、図５０の形式では空白が多くなってしまい、

却って効率が悪くなる。従って、放送受信装置の実装上は図４９、図５０の両方の形式にも対応している課金制御部１１０６が一般的な意味で望ましい。このためには、両方の形式のバケットを情報識別子で区別し、それに対応した処理部を用意すれば良い。

【０２６０】受信契約情報に前記認証子を含めると受信契約情報は、図７５のような形式になり、前記デジタル署名を含めると受信契約情報は、図７６のような形式となる。また、これらに、図４９、図５０の契約情報バケットの形式を適用することも可能で、その場合はそれぞれ図７７、図７８のような形式となる。また、当然情報の順序に関しては（受信装置の設計段階で決めておく必要はあるものの）特に制約はなく、図７４～図７８に示す形式にあっては要素毎に順序を変えたバリエーションは存在する。

【０２６１】また、これら複数の形式を混在させて送る場合は、図３７に示したように、さらに、情報識別子で識別し、それに対応した処理部を用意すれば良い。

【０２６２】２）契約管理装置

次に、図３１のに示した構成の放送受信装置に対応する、情報配信側の契約管理装置について説明する。

【０２６３】図７０は、本実施形態に係る契約管理装置の構成例を示したもので、本実施形態に示した機能を全て実現したものであり、実現されるシステムにおいて不必要な機能がある場合にはその部分の構成を削ることができる。

【０２６４】なお、図７０において、契約ユーザＤＢ２００１、支払い確認待ちＤＢ２００２、契約期間確認部２００７、契約情報ＤＢ２００５、スケジューリング部２０１４、放送装置２０１３、契約情報バケット出力要請部２０１２、シードＤＢ２００３、シード・マスター鍵生成部２０１０は、図３の契約管理装置における契約ユーザＤＢ１、支払い確認待ちＤＢ２、契約期間確認部７、付加情報ＤＢ５、スケジューリング部１４、放送装置１３、付加情報出力要請部１２、シードＤＢ３、シード・マスターキー生成部１０と同様であるので、説明は要略し、本実施形態に特徴的な部分についてのみ説明する。

【０２６５】なお、図７０において、契約変更ユーザＤＢ２００６には、所定期間内に契約内容を変更した（新規契約も含まれる）ユーザに関する情報（例えば、受信装置ＩＤ、チャンネル番号等のチャネル契約情報等）が書き込まれるものである。

【０２６６】図７０に示した契約管理装置で特徴的な部分は、契約情報バケット生成部２００８である。契約情報バケット生成部２００８の構成例を図７２に示し、図７３に示したフローチャートを参照して、契約情報バケット生成部２００８の構成と処理動作について説明する。

【０２６７】契約情報バケット生成部２００８は、契約管理装置の契約情報バケット制御部２００９からの命令を受信契約情報作成部２０３２で受け、動作を開始する（ステップＳ１１３１）。受信契約情報作成部２０３２に送られる命令としては、例えば、「１９９８年７月１５日に送信予定の最近２ヶ月間に契約変更した契約者の契約情報を順次作成せよ」というような内容である。このような命令を受けた受信契約情報作成部２０３２では、契約ユーザ情報検索／入力部２０３１を介して、契約変更ユーザＤＢ２００６、場合によっては契約ユーザＤＢ２００１を検索し、該当するユーザの情報を順次抽出する（ステップＳ１１３２～ステップＳ１１３３）。

【０２６８】次に、チャネルキー復号鍵検索／入力部２０３８を介して、チャネルキー復号鍵ＤＢ２０１６から送信時期に対応したチャネルキー復号鍵を検索し（ステップＳ１１３４）、図７４に示すような第１の中間データを生成する（ステップＳ１１３５）。

【０２６９】次に、認証子生成部２０３６にて、該第１の中間データに対して認証子を作成し（ステップＳ１１３６）、それを該第１の中間データに付加して、図７５に示すような第２の中間データを作成する。更に、ディジタル署名用鍵検索／入力部２０３７を介してデジタル署名用鍵ＤＢ２０１７から送信時期に対応したデジタル署名用の秘密鍵を検索し、該秘密鍵でデジタル署名を作成し（ステップＳ１１３７）、該デジタル署名を第２の中間データに付加して、図７６に示すような受信契約情報を作成する（ステップＳ１１３８）。

【０２７０】ここで、デジタル署名の対象とするデータは第１の中間データだけであっても良いし、第２の中間データであってもよい。一般に後者の方がより強いセキュリティを実現できる。

【０２７１】次に、受信契約情報を暗号化部２０３３に送り、暗号化部２０３３では、マスター鍵検索／入力部２０３９を介して、マスター鍵ＤＢ２０１５から放送時期に合ったマスター鍵をマスター鍵ＤＢから検索抽出し（ステップＳ１１３９）、それを使って受信契約情報を暗号化する（ステップＳ１１４０）。

【０２７２】契約情報バケット作成部２０３４では、暗号化された受信契約情報にチャネルキー復号鍵識別子、マスター鍵識別子、情報識別子を付加して、例えば、図３７に示すような契約情報バケットを作成する（ステップＳ１１４１）。契約情報バケットを作成するには、図３７に示したように、チャネルキー復号鍵識別子、マスター鍵識別子、情報識別子を付加すれば良いが、前２者はそれぞれのデータベースから取得でき、情報識別子に関しては契約情報バケットに対して予め割りふられた識別子を付加すれば良い。

【０２７３】また、図４９に示すような受信契約情報（もしくは第１の中間データ）を作成することも同様に可能である。更に図５０に示すような圧縮された受信契約情報（もしくは第１の中間データ）を作成することも

可能であるが、この場合、契約ユーザ情報検索／入力部２０３１での処理が複雑になる。即ち、契約ユーザ情報検索／入力部２０３１は、同じチャネル契約情報を持った契約者を検索する必要がある。ここで契約の種類が少なければ図５０に示すような圧縮された契約情報は有効であるが、契約の種類が多い場合は無駄な領域が増えてしまうので送信量が多くなり不利になる。そこで、図４９の形式と図５０の形式をチャネル契約情報に応じて取り混ぜて送る必要もある。この場合どちらの形式にするかを決定するのは受信契約情報作成部２０３２であり、受信契約情報作成部２０３２では、契約ユーザ情報検索／入力部２０３１の検索結果に基づいて決定する。例えば、図４９の形式に入るチャネル契約情報の数が１０で、図５０の形式に入るチャネル契約情報の数が２０である場合、受信契約情報の作成条件に合う契約者のうち同じチャネル契約情報を持つ契約者が１０件以下であれば図４９の形式、１１件以上であれば図５０の形式とするなどと処理することができる。更に２つの形式の違いをパケット上で明示しなくては、放送受信装置側で処理ができないが、これには情報識別子を利用すれば良い。即ち、契約情報パケットの形式によって複数の情報識別子を使い分けることになる。もちろんこのことは、契約情報パケットが取り得る様々な形式に対して適応することができる。例えばデジタル署名の有無、認証子の有無などは契約情報を図４９の形式にするか図５０の形式にするかという事柄とは独立であり、どのオプションを取った契約情報パケットであるかを明示することにも情報識別子を利用することができる。

【０２７４】最後に契約情報の送出スケジュールについて述べる。本発明は、契約情報の送出に使える帯域が狭くて同等の安全性が保証できることが有意点であることから、以下で述べる契約者毎に契約情報の送出頻度を変化させる送信方式は意義が深い。即ち、契約変更者は契約変更の内容にもよるが（特に不利な契約情報の場合は）なるべく受信せずに視聴し続けようとして受信契約情報の受信拒否をすることが考えられる。ここで言う受信拒否は毎日短時間しか視聴しないか、一定期間スイッチをオフにしておく等の単純なものである。

【０２７５】このような意味からは契約変更後に、契約情報を送る期間を一定なものにすると限定受信が実現できない可能性がある。例えば、契約変更後１年間しか契約情報を送らないとしてしまうと、契約変更後１年間１度も放送受信装置にスイッチを入れないと（契約情報は取得できないので）契約情報が更新されず、それ以降古い契約情報のまま視聴し続けられてしまうことになる。

【０２７６】一方で契約変更後、受信契約情報を半永久的に送り続けることにすると、既に受信した契約者の分を何度も送信することになるので放送帯域が有効に使えない。そこで、契約変更後の経過時間毎に契約情報の送信頻度を変化させる必要が生じる。契約情報の送信頻度の一例を以下に示す。

・　契約変更後の経過時間が２ヶ月のとき　…送信頻度は１０分に１回
・　契約変更後の経過時間が２ヶ月～６ヶ月のとき…送信頻度は３０分に１回
・　契約変更後の経過時間が６ヶ月～１年のとき　…送信頻度は６０分に１回
・　契約変更後の経過時間が１年以上のとき　…送信頻度は１２０分に１回

ここでは、最初の２ヶ月は１０分に１回送信し、早期の契約変更を目指す。大多数の受信装置はこの段階で契約変更がなされると考えられるが、たまたま受信できなかったか長期間スイッチをオフしていたため契約情報を受信できなかった受信装置のために、その後も２ヶ月経過後から６ヶ月経過後までに３０分に１回、６ヶ月経過後から１年経過後まで６０分に１回、１年経過後以降は１２０分に１回という形で送信頻度を下げて送り続けることにより、放送帯域を節約しながら確実な限定受信を行うことができる。

【０２７７】一方、新規契約者に対しては、契約者自身早期に受信したいと望むし、万が一契約情報が（何らかの原因で）受信できなかった場合でも、後日クレームという形で放送局側にフィードバックがかかるので、このとき再送信すればよく、長期間にわたって送信する意味はあまりない。この意味から新規契約者については、新規契約後２ヶ月間だけ１０分に１回程度の頻度で送信すれば足りると考えられる。

【０２７８】以上のように、契約の種類（例えば、契約変更、新規契約など）と契約後の経過期間によって、契約情報の放送頻度を変更する送信スケジュールが望ましい。本実施形態の契約管理装置にあっては、契約情報パケット生成制御部が例えば上記の頻度で送信するように調整する。

【０２７９】（第４の実施形態）

１）放送受信装置

図５１は、本実施形態に係る放送受信装置の構成を概略的に示したものである。本実施形態は第３の実施形態を同レベルのセキュリティを保ったまま簡略化したものである。従って、図３１と同一部分には同一符号を付し、異なる部分について説明する。

【０２８０】本実施形態が第３の実施形態と本質的に異なるところは、図３１のチャネルキー復号部１１０９がないことである。従って、図５２に示すように、暗号化された放送コンテンツを復号するための鍵構成が３段になっている。

【０２８１】また、本実施形態ではチャネルキーは受信契約情報の中に含まれる。したがって通常チャネルの情報は、図５３に示すように、スクランブルされたコンテンツ情報のみとなる。それに伴い、契約情報チャネルにて配信される契約情報パケットも図５４のようになり、

チャネルキー復号鍵の代わりにチャネルキーが入るためチャネルキー識別子と対応するチャネル識別子が必要になる。

【０２８２】受信契約情報は、図５５に示したように、受信装置ＩＤ、チャネル契約情報、チャネルキーから構成される。この受信契約情報も第３の実施形態で述べたように図４９に示したのと同様なパッキングが可能である。また、図５４に示す契約情報バケットではチャネル識別子が未暗号化部分にあるため、選択しているチャネルのチャネル識別子に対応した契約情報のみを取得することが可能となる。これを避けるため、図５７に示すように、受信契約情報中に、チャネル識別子とチャネルキー識別子を含めて、これ全体を暗号化する構成を考える。この場合、契約情報バケットは、図５６に示すように、暗号化された受信契約情報とマスター鍵識別子と情報識別子を含む構成となる。

【０２８３】さらに、受信契約情報が図５８に示すような構成であるとすると、受信契約情報には、チャネルキー「０」とチャネルキー「１」が存在し、どちらかが現在の放送コンテンツの復号鍵であり、もう一方が次に有効になる鍵とすることができ、チャネルキー識別子が要らなくなる。

【０２８４】更に、第３の実施形態に示した受信契約情報と同様に、受信契約情報に認証子やデジタル署名を付加することができ、付加した場合、第３の実施形態と同様の効果がある。例として最も受信契約情報が複雑になる場合、即ち、図４９、図５０の形式で受信契約情報を記述し、図５８のように２つのチャネルキーを含めた例を図７９、図８０にそれぞれ示す。また、情報の順序に関しては第３の実施形態と同様で、特に制約はなく、データ毎に順序を変更することは可能である。また、これら複数の形式を混在させて送る場合は情報識別子で識別すれば良い。

【０２８５】さて、契約情報受信時は契約情報バケットがフィルター部１１０７で分離され契約情報復号部１１１０に送られる。その中に含まれる暗号化された受信契約情報を対応するマスター鍵を用いて復号し、受信契約情報に含まれる受信装置ＩＤを（複数ある場合は）順次検索して行き、当該受信装置のＩＤが見つかった場合は、それに対応するチャネル契約情報をチャネル契約情報格納部１１１６へ格納する。同時に、受信装置ＩＤが当該受信装置である無しに関わらず、受信契約情報に含まれるチャネルキーを、該受信契約情報にて示されたチャネル識別子とチャネルキー識別子の組合せに対応させて、図５９のように、メモリ（図５１のチャネルキー格納部１１１７）に書き込む。

【０２８６】チャネルキー出力部１１２０はデスクランブル部１１０８からの要請により契約判定部１１１８での判定にしたがって、チャネルキー格納部１１１７から対応するチャネルキーを検索して、デスクランブル部１１０８に出力する。

【０２８７】ここでは、図５９に示したように、取得した全てチャネルキーをチャネル識別子とともにチャネルキー格納部１１１７に格納している。しかし、これは同時に視聴するチャネルは高々１つであるため必ずしも必要はない。そこで認証部１１１４で現在視聴しているチャネル番号を参照し、必要なチャネルキーだけをチャネルキー格納部１１１７に格納することも可能である。この場合、チャネルキー格納部１１１７には、図４１に示したように、チャネルキーとその識別子とが格納される。この構造を取った場合、チャネル変更時にはチャネルキー格納部１１１７の内部をクリアしなくてはならない。何故なら変更後のチャネルのチャネルキーは変更前のチャネルのチャネルキーとは一般的に異なるので、格納部をクリアしないと変更前のチャネルのチャネルキーが有効になってしまい、意味不明の放送コンテンツが出力されることになるからである。このようにすることによって、チャネル変更時には、チャネルキー格納部１１１７をクリアしてチャネル契約情報から新たにチャネルキーを取得しなくてはならないため、デスクランブルまでに処理時間がかかるが、チャネルキー格納部１１１７のメモリ容量が少なくて済み、また、チャネル数が増えてもメモリ容量を増やすなどの処置をしなくても良い。

【０２８８】このような方式を実現するためには、認証部１１１４がチャンネル情報入力部１１１９からチャネル番号を取得する必要があり、図５１の点線で示したようなデータの流れが更に必要である。

【０２８９】また、本実施形態の方式を取ることにより、第３の実施形態と比較して鍵構成を１段減らせることによるメリット以外にも、次のようなメリットがある。すなわち、全チャネルを１ヶ月分契約した契約者が次の月に全てのチャンネルを解約したとする。この場合、この契約者は自分の放送受信装置宛の新しい受信契約情報を取得したくない。何故なら取得すると全チャンネルが視聴できなくなってしまうからである。しかし、受信契約情報の中には放送コンテンツの復号のために必要な情報があるのでその全てを取得しない訳にはいかない。第３の実施形態の場合は、必要な情報はチャネルキー復号鍵K_Hであった訳であるが、これは全チャネルに対して共通であるのでチャネルキー復号鍵K_Hが変更されるタイミング に対し、高々１つの受信契約情報を取得すれば良い。もし、K_Hの変更が１日に １回であれば、自分の放送受信装置宛ての受信契約情報を受け取らないことも十分に可能である。これに対して、本実施形態では必要な情報はチャネルキーそのものであり、しかもチャネルキーはチャネル毎に異なり、安全性の必要上頻繁に変更する必要がある。このため、受信契約情報もかなり頻繁に取得する必要に迫られ、自分の放送受信装置宛ての受信契約情報を受け取らない確率はかなり低くなる。

【０２９０】だが、第３の実施形態の４段の鍵構成にも積極的に採用するに足る意義がある。もし、チャネルが多く（例えば１０００チャンネル）あった場合、受信開始時もしくはチャネル変更時にかなりの数（最悪１０００個）の受信契約情報を取得して復号した後でないと、当該チャネルのチャネルキーは取得できない。これでは受信のタイミングがかなり遅くなって実用に耐えないばかりか、万一受信誤りが生じた場合がもう１０００個復号するまで待たなくてはならない。この点を解消したのが４段の鍵構成である。

【０２９１】４段の鍵構成の場合、チャンルキー復号鍵という全ての放送受信装置に共通の鍵があり、全てのチャネルキーがそれで復号されるためチャネルの数に依らず一定の時間で復号できる。これらの利点を生かして、構成された放送受信装置の構成例を図６０に示す。ここでは、契約情報バケットおよび受信契約情報のフォーマットを２種類用意し、１つは第３の実施形態で示した図３７、図３８のようなものであり、他の１つは本実施形態に係る図５４、図５５のようなものである。

【０２９２】これらの違いを契約情報バケット中の情報識別子で判断し、認証部１１１４では、受信契約情報中に含まれているものがチャネルキー復号鍵であれば、チャネルキー復号鍵格納部１１１５へ、チャネルキーであればチャネルキー格納部１１１７へ送る。

【０２９３】なお、受信契約情報にチャネルキー復号鍵が含まれる時には、通常チャネルにて別途チャネルキー情報を送り、そうでない時にはチャネルキー情報を送らないように放送局（契約管理装置）側で調整する。このため両方の回路が混在しても矛盾なく動作することができる。

【０２９４】２）契約管理装置

次に、本実施形態に係る放送受信装置に対応する、情報配信側の契約管理装置について説明する。

【０２９５】図７１は、本実施形態に係る契約管理装置の構成例を示したもので、本実施形態に示した機能を全て実現したものであり、実現されるシステムにおいて不必要な機能がある場合にはその部分の構成を削ることができる。なお、図７１に示した契約管理装置において、図７０に示した第３の実施形態における契約管理装置と同一部分には、同一符号を付し、異なる部分について説明する。すなわち、図７０のチャネルキー復号鍵ＤＢ２０１６とチャネルキー復号鍵生成部２０１８が図７１では、それぞれ、チャネルキーＤＢ２０２１、チャネルキー生成部２０２２に置き換えられ、図７１のチャネルキーＤＢ２０２１、チャネルキー生成部２０２２の処理動作の説明は、図７０のチャネルキー復号鍵ＤＢ２０１６とチャネルキー復号鍵生成部２０１８の説明部分において、チャネルキー復号鍵をチャネルキーと置き換えれば、同様である。

【０２９６】（第５の実施形態）第５の実施形態では、第１～第４の実施形態の限定受信システムに共通に利用可能で、放送受信装置内にある課金制御部１１０６のテスト用ラッチ部の構成に関する実施形態を示すものである。図６１に、本実施形態に係る放送受信装置の構成例を示す。

【０２９７】受信限定システムは、その構成上、課金制御部１１０６の内部の秘密情報（特にマスター鍵生成の鍵やアルゴリズム）が露見すると、システム全体が破綻し、有効な課金ができなくなる危険がある。また、例えば図３１において出力されたデスクランブルされた放送コンテンツが何らかの手段でユーザに記録されるとそれを何回でも再生することが原理的にできてしまい好ましくない。その意味から課金制御部１１０６とその出力を利用するＭＰＥＧデコーダは一体化されたチップで構成されていることが好ましい。

【０２９８】一方、一体化されたチップを作成する際は１回で正しいチップを作成することは困難なので中間結果をテストピンなどを通して見てみる必要がある。また、このテストピンは製品段階でも残ってしまうので、本チップを解析しようとする者に対して復号プロセスを中間結果といえども観察できる機会を与え、暗号アルゴリズムや復号鍵の解析に都合の良い状況を作り出してしまう。そこで考えられたのが本実施形態である。

【０２９９】上記目的を達成するために、第１～４の実施形態に示した放送受信装置に付加するものは、図６１に示すように、スキャンパステスト用ラッチ部１２０１、１２０３と、スキャンパス出力部１２０２、１２０４である。

【０３００】スキャンパステスト用ラッチ部１２０１、１２０３は、そこを流れるデータを捕え、それぞれスキャンパス出力部１２０２、１２０４へ送る動作を行う。

【０３０１】１）スキャンパステスト用第１のラッチ部（受信契約情報のテスト出力）

図６２に、スキャンパステスト用第１のラッチ部１２０１の基本的な構成例を示し、図６３に示すフローチャートを参照しながらスキャンパステスト用第１のラッチ部１２０１の構成およびその処理動作について説明する。

【０３０２】スキャンパステスト用第１のラッチ部１２０１では、契約情報復号部１１１０からの出力（復号された受信契約情報）を入力部１３０１で受取り（ステップＳ１１０１）、そのデータを（必要があれば）データフォーマットの変更などを行い認証部１３０２へ送る。認証部１３０２では、当該情報を出力しても良いか否かの判定を行う（ステップＳ１１０２）。もし、出力しても良いと判定された場合、当該データを出力部１３０５へ送り（ステップＳ１１０３）、出力部１３０５は、第１のスキャンパス出力部１２０２へ送る（ステップＳ１１０４）。第１のスキャンパス出力部１２０２は、当該データを課金制御部１１０６外へ出力し、当該データは課金制御部１１０６外にあるディスプレイ装置等の表示

部に表示される（ステップＳ１１０５）。

【０３０３】認証部１３０２にて、ステップＳ１１０５の処理に続いて、あるいは、復号された受信契約情報を出力しないと判定したとき、当該復号された受信契約情報をそのままスキャンバステスト用第１のラッチ部１２０１の外部にある認証部１１１４へ出力する（ステップＳ１１０６）。

【０３０４】ここで、認証部１３０２の働きは重要である。以下では認証部１３０２の働きを説明するため、課金制御部１１０６への入力データフォーマットに立ち戻って説明する。まず簡単のため最も単純な実現方法を示す。第３、第４の実施形態における契約情報バケットの構成（図３７、図５４参照）にある情報識別子として、通常の（受信契約情報を示す）識別子以外にスキャンバス出力が可である受信契約情報である旨を示す識別子を設ける。この情報識別子を認証部１３０２で判断することによって当該データを第１のスキャンバス出力部１２０２に出力するか否かを決定するのである。

【０３０５】スキャンバス出力をさせる必要があるのは、基本的に設計時もしくは工場出荷時であるので、スキャンバス出力を可にする情報識別子は放送波では流さないと考えて良く、当該情報識別子がどういうものかを一般のユーザが解析するのは困難である。

【０３０６】次に、スキャンバス出力が可である受信契約情報を含む契約情報バケットであるか否かを、契約情報バケットに対応した認証情報で判定する例を示す。この場合の契約情報復号部１１１０へ入力する契約情報バケットのフォーマットを図６４に示す。

【０３０７】図３７と異なるのは、暗号化された受信契約情報に続いて認証情報がさらに加わった点である。勿論、図５４の場合も図６４と同様に変更すればよい。なお、（認証情報がない）通常のフォーマットの契約情報バケットと区別するために、そのための情報認証子を別に設定するか、情報識別子を共通にした場合は、フォーマットをそろえるため、通常の契約情報バケットにおける認証情報は「ＮＵＬＬ」として、「ＮＵＬＬ」の認証情報バケットが来た場合は通常の契約情報バケットであると解釈しても良い。但し、後者の場合は実装が簡単だが、データ量が多くなるという欠点がある。

【０３０８】認証情報として、例えば暗号化された受信契約情報（もしくはそのハッシュ値）に電子署名を施したものを考える。ここでデータのハッシュ値とは任意長のデータを一定の長さ（例えば１２０ビット）で表現したデータのダイジェストのようなものである。ダイジェストといっても内容そのものの要約ではなく、データにハッシュ値と呼ばれる何らかの一方向性関数（逆関数を求めることが困難な数学的関数）を施して、一定の長さにしたものと言うことができる。このようなハッシュ関数はＭＤ５やＳＨＡ１などいくつか知られている。電子署名を付けるデータは暗号の１ブロックにあたる６４ビットもしくが１２０ビットの一定の長さにしておく必要がある。このため必要があれば受信契約情報にハッシュ関数を掛ける。

【０３０９】スキャンバステスト用第１のラッチ部１２０１が、復号された受信契約情報とともに、認証情報と暗号化された受信契約情報も受取り、認証情報としての電子署名を確認する、確認のプロセスを含めたスキャンバステスト用第１のラッチ部１２０１の処理動作について、図６６に示すフローチャートを参照しながら説明する。

【０３１０】入力部１３０１には、復号された受信契約情報とともに、認証情報と暗号化された受信契約情報も受取り（ステップＳ１１２１）、認証部１３０２では、電子署名の確認のためにはまず（入力された）暗号化された受信契約情報に（必要に応じて）ハッシュ関数を掛ける（ステップＳ１１２２）。一方、認証部１３０２に予め格納されている公開鍵で認証情報としての電子署名を復号し（ステップＳ１１２３）、前記ハッシュ値と比較する。ここで一致していれば（ステップＳ１１２４）、認証情報は正しいと考えることができ、図６３のステップＳ１１０３～ステップＳ１１０５と同様にして、データの出力を行う（ステップＳ１１２５～ステップＳ１１２７）。

【０３１１】ステップＳ１１２４で、一致していなければ、当該認証情報は正しくないと判定して、データの出力は行わない（ステップＳ１１２８）。ステップＳ１１２７の処理に続いて、あるいは、認証情報とハッシュ値とが一致しないとき、当該復号された受信契約情報をそのまま、スキャンバステスト用第１のラッチ部１２０１の外部にある認証部１１１４へ出力する（ステップＳ１１２８）。

【０３１２】ここで、公開鍵暗号を使った電子署名はデータ本体（ここではハッシュ値）に対して秘密鍵で暗号化したものを言う。公開鍵暗号において秘密鍵で暗号化したものは公開鍵といわれる秘密鍵とは別の鍵でなくては復号できない。このため電子署名を公開鍵で復号すれば元のハッシュ値になるはずである。また、公開鍵暗号の安全性から公開鍵で復号できるようなデータを作成できるのは秘密鍵を知っている人だけと考えられるので、ハッシュ値を秘密鍵で暗号化したデータを当該データの電子署名と呼んでいる。ここで公開鍵暗号を使った電子署名を使う意義は、課金制御部１１０６内の情報だけでは電子署名を作成できないので一般者がスキャンバステスト用ラッチ部１２０１、１２０３に対して出力させるようなデータを作成するのは事実上不可能である点である。また、電子署名は共通鍵暗号を使っても可能となる。この場合ハッシュ値を共通鍵で暗号化し、共通鍵で復号することによって確認するので、共通鍵は当該ラッチ部に秘匿しておかなくてはならない。しかし、共通鍵暗号は公開鍵暗号に比べて高速であるという特徴があ

り、このための共通鍵は課金チップという耐タンパはハードウェア上に隠されているので、読み取るのは極めて困難である。このことから共通鍵による電子署名も有効である。

【０３１３】暗号化された電子署名を確認するため、スキャンパステスト用第１のラッチ部１２０１には、本来必要のない暗号化された受信契約情報を入力している。これを避けるためには契約情報復号部１１１０で電子署名を検証し、その結果をスキャンパステスト用第１のラッチ部１２０１に送るという方法が考えられる。即ち、スキャンパステスト用第１のラッチ部１２０１の認証部１３０２の主要部分を契約情報復号部１２０１で行なうという訳である。だが、この方法ではラッチ部に対して出力を促すデータは常に同じであり、第３者による悪用を許しやすい。

【０３１４】その意味で契約情報復号部１１１０で署名が認証された場合、契約情報復号部１１１０でその出力に電子署名を施すという実現方法もある。この方法によれば前記の悪用の問題は避けられるが、処理が余分にかかる。いずれの方法を取るかはアプリケーションの性質によって決まる。

【０３１５】次にスキャンパステスト用第１のラッチ部１２０１が出力するデータについて考えてみると、前記の全ての例では生のデータ列（０、１の列）、すなわち、復号された契約受信情報そのものが出力される。もしデータ列が暗号化されていれば、更に安心である。即ち、例えスキャンパステスト用第１のラッチ部１２０１から無条件でデータが出力されてもそのデータが暗号化されており、復号鍵を備えた表示装置でないと復号できないような構成にしていれば当該ラッチ部１２０１の出力から課金制御部１１０６の構成を解析することは極めて困難である。

【０３１６】このようなスキャンパステスト用第１のラッチ部１２０１の構成例を図６６にに示す。図６６において、暗号化部１３０３に公開鍵暗号を導入して、公開鍵で暗号化するようにすれば更に安全である。何故なら暗号化された出力データは課金制御部１１０６内には含まれない秘密鍵でしか復号できないからである。しかし、実際は処理時間の観点で共通鍵暗号を使われる機会が多いだろう。この場合共通鍵を暗号化鍵格納部１３０４に秘匿しておく必要がある。さもないと、せっかく暗号化しても第三者に共通鍵が露見すれば復号されて、出力内容が露見してしまうからである。

【０３１７】２）スキャンパステスト用第２のラッチ部（受信装置ＩＤのテスト出力）

次に、図６１のスキャンパステスト用第２のラッチ部１２０３について説明する。スキャンパステスト用第２のラッチ部１２０３の動作も前述の第１のラッチ部１２０１と基本的には同じであるが、第１のラッチ部１２０１がいわばデータが一方向に通り過ぎるだけであったのに対し、第２のラッチ部１２０３は受信装置ＩＤ格納部１１１３から受信装置ＩＤの読み込みを行い、その結果をラッチするのであるから構成が多少複雑になる。

【０３１８】この第２のラッチ部１２０３は、受信装置ＩＤが、例えば、不揮発性メモリにて構成されている受信装置ＩＤ格納部１１１３に正しく格納されているかを確認するためのものである。

【０３１９】図６７にスキャンパステスト用第２のラッチ部１２０３の構成例を示す。

【０３２０】認証部１１１４からのデータは、スキャンパステスト用第２のラッチ部１２０３の第１の入力部１４０１で受取り、認証部１４０２へ送られる。認証部１４０２は、前述の第１のラッチ部１２０１の認証部１３０２と同様に、入力結果に対するラッチ出力の可否に関する認証を行う。

【０３２１】認証結果は認証結果格納部１４０３に格納される。一方、認証部１４０２から受信装置ＩＤ格納部１１１３へは、受信装置ＩＤの出力を要請する命令を流す。それを受け取った受信装置ＩＤ格納部１１１３は、受信装置ＩＤを出力し、第２の入力部１４０５へそれを入力する。受信装置ＩＤはラッチ出力可否判定部１４０４へ送られ、ラッチ出力可否判定部１４０４では、認証結果格納部１４０３にある認証結果を参照して、認証されている場合には、受信装置ＩＤを第２のスキャンパス１２０４へ出力する。

【０３２２】なお、ラッチ出力可否判定部１４０４は、認証部１４０２で認証されている場合でもされていない場合でも、受信装置ＩＤ格納部１１１３から受け取った受信装置ＩＤは外部の認証部１１１４へ出力する。

【０３２３】また、ラッチ出力可否判定部１４０４の後段に、図６６に示したような暗号化部１３０３、暗号鍵格納部１３０４を付け加えれば、前述同様、受信装置ＩＤを暗号化して出力することもできる。

【０３２４】（第６の実施形態）

１）放送システムの概略

放送受信装置に受信契約情報を放送配信する以外に、磁気カード等の形態可能な記録媒体（以下、簡単にカードＰと呼ぶ）に記録し、それを当該放送受信装置に宅配又は郵送する点が、前述の第３～第５の実施形態の場合と異なる。契約ユーザは、放送受信装置に受け取ったカードＰに記録された情報を読み取らせることにより、契約チャネルの受信が可能となる。

【０３２５】ここでは、第３の実施形態の契約管理装置（図７０参照）、放送受信装置（図３１）に対応した契約管理装置（図８１参照）、放送受信装置（図８２参照）を例にとり説明するが、他の実施形態に係る契約管理装置、放送受信装置も、基本的には同様である。すなわち、第６の実施形態に係る契約管理装置では、第３～第５の実施形態に係る契約管理装置の放送装置２０１３がカード作成部２０５１に置き換えられ、あるいは、さ

らに追加されている。カード作成部２０５１は、契約ユーザのカードＰに暗号化された受信契約情報を書き込むようになっている。また、第６の実施形態に係る放送受信装置では、契約情報復号部１１１０に、カードリーダ２０６１に挿入されたカードＰから読み取られた暗号化された受信契約情報が入力するようになっている。

【０３２６】２）契約管理装置

図８１は、第６の実施形態に係る契約管理装置の構成例を示したもので、図７０と同一部分は同一符号を付し、異なる部分について説明する。すなわち、図７０の受信装置毎の受信契約情報を地上波あるいは衛星放送を介して配信するための放送装置２０１３が図８１では、カード作成部２０５１に置き換えられ、あるいは、さらに追加して必要に応じて適宜切り替えられるようになっている。

【０３２７】カード作成部２０５１により、カードＰに、そのカードＰに対応した受信装置の契約期間に応じた受信契約情報等を記録して、契約ユーザに配布するようになっている。

【０３２８】例えば、１９９７年１２月１日から４ヶ月間契約している契約ユーザに対しては、マスターキーが１ヶ月毎に更新されるとき、受信契約を１ヶ月毎に作成しなくてはならないために１ヶ月毎に有効なチャネルキー復号鍵と有効なマスターキーを検索して、図７３のフローチャートに示す処理を行う必要がある。図８１に示す契約管理装置では、受信契約情報を放送によらずに例えばカードＰに４ヶ月分の契約チャネルのチャネルキー復号鍵に対応する受信契約情報を書込み、当該ユーザに配送すればよい。これにより、１ヶ月毎の配信、配布を行わなくてもよく、放送局側にもユーザ側にも煩雑を避ける意味で有利である。

【０３２９】ところで、受信契約情報を作成するためには、契約管理装置は、契約ユーザの購入した放送受信装置の受信装置ＩＤを知る必要がある。もちろん、この受信装置ＩＤは、各放送受信装置内の耐タンパな受信装置ＩＤ格納部１１１３に書き込まれているため、外部からの読取りは不可能である。従って、契約管理装置に契約ユーザの購入した放送受信装置の受信装置ＩＤを入力するための手段が必要になってくるであろう。

【０３３０】そこで、次に、契約管理装置に、購入された放送受信装置の受信装置ＩＤを入力するための一手段を説明する。

【０３３１】例えば、購入された放送受信装置の筐体や包装用のバッケージ等に当該放送受信装置の表層受信装置ＩＤ（受信装置ＩＤに１対１に対応するような識別子で、例えば、受信装置ＩＤそのものを暗号化したものであってもよい）を印刷する。図８１に示したように、契約管理装置に入力部２０７２、表層受信装置ＩＤ変換部２０７１を新たに設ける。

【０３３２】契約情報入力部２０７２からは、契約時、ユーザの契約情報と当該ユーザの購入した放送受信装置の表層受信装置ＩＤを入力するものとする。この入力には、例えば、スキャナ等を用いてもよく、特に限定しない。

【０３３３】表層受信装置ＩＤ変換部２０７１には、予め、表層受信装置ＩＤと受信装置ＩＤとの対応関係を示した変換テーブル２０７３を記憶している。

【０３３４】契約情報入力部２０７２に入力された表層受信装置ＩＤは、表層受信装置ＩＤ変換部２０７１に渡され、ここで、変換テーブル２０７３を参照して、表層受信装置ＩＤから受信装置ＩＤへ変換し（すなわち、変換テーブル２０７３から表層受信装置ＩＤに対応する受信装置ＩＤを検索する）、その結果得られた受信装置ＩＤを支払確認待ちＤＢ２００２に渡す。

【０３３５】一方、契約情報入力部２０７２に入力された契約情報は、支払確認待ちＤＢ２００２に渡される。支払確認待ちＤＢ２００２は、当該契約情報を、表層受信装置ＩＤ変換部２０７１から受け取った受信装置ＩＤに対応させて登録する。

【０３３６】その後の支払確認待ちＤＢ２００２に対する処理動作は、図３の支払確認待ちＤＢ２と同様である。

【０３３７】２）受信装置

図８２は、第６の実施形態に係る放送受信装置の構成例を示したものである。なお、図３１と同一部分には同一符号を付し、異なる部分について説明する。すなわち、前述の図８１に示したような放送局側に設置されている契約管理装置で作成されたカードＰから暗号化された受信契約情報を読み取るためのカードリーダ２０６１がさらに追加されて、カードリーダ２０６１にてカードＰから読み取られた暗号化された受信契約情報は、契約情報復号部１１１０に入力される。

【０３３８】なお、その後の動作は、第３の実施形態と同様である。

【０３３９】

【発明の効果】以上説明したように、本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信が実現できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態（付加情報を放送配信する場合）に係る契約管理装置および放送受信装置を用いた放送システムの概略構成を示した図。

【図２】図１に示した放送サービスへの加入・継続契約時、契約更新時、解約時、課金手続きの概略的に流れを示した図。

【図３】第１の本実施形態に係る契約管理装置の構成例を示した図。

【図４】契約管理装置の契約ユーザＤＢのデータ記憶形

式の一例を示した図。
【図５】契約管理装置のシードＤＢのデータ記憶形式の一例を示した図。
【図６】契約管理装置のチャネルＤＢのデータ記憶形式の一例を示した図。
【図７】契約ユーザへ登録処理を説明するためのフローチャート。
【図８】契約管理装置の処理動作（契約ユーザ毎に対応した付加情報を生成し、これを配信するまでの手順）を説明するためのフローチャート。
【図９】（ａ）図は主にコンテンツを配信するための放送波に多重される情報の一例を概念的に示した図で、（ｂ）図は付加情報のデータ形式の一例を示した図。
【図１０】コンテンツ情報の配信装置の構成例を示した図。
【図１１】（ａ）図は主にコンテンツを配信するための放送波に多重される情報の他の例を概念的に示した図で、（ｂ）図は付加情報のデータ形式の他の例を示した図。
【図１２】端末付加情報のデータ形式の一例を示した図。
【図１３】チャネル付加情報のデータ形式の一例を示した図。
【図１４】第１の実施形態に係る受信装置の構成例を示した図。
【図１５】図１４の受信装置の処理動作を説明するためのフローチャート。
【図１６】図１４の受信装置の処理動作を説明するためのフローチャート。
【図１７】図１４の受信装置の処理動作を説明するためのフローチャート。
【図１８】図１４の受信装置の処理動作を説明するためのフローチャート。
【図１９】新規契約に関する付加情報（ＯＮ信号）の送信量と、解約に関する付加情報（ＯＦＦ信号）の送信量の時間経過に伴う変動を示した図。
【図２０】付加情報の受信状況を監視する処理を伴う場合の受信装置のフィルタの処理動作を説明するためのフローチャート。
【図２１】端末付加情報とチャネル付加情報とを用いた場合の図１４の受信装置の処理動作を説明するためのフローチャート。
【図２２】端末付加情報とチャネル付加情報とを用いた場合の図１４の受信装置の処理動作を説明するためのフローチャート。
【図２３】端末付加情報とチャネル付加情報とを用いた場合の図１４の受信装置の処理動作を説明するためのフローチャート。
【図２４】本発明の第２の実施形態（付加情報をカード型記録媒体に記録して顧客に配布する場合）に係る放送システムの概略構成を示した図。
【図２５】第２の実施形態に係る契約管理装置の構成例を示した図。
【図２６】第２の実施形態に係る受信装置の構成例を示した図。
【図２７】カード型記録媒体に記録される付加情報の一例を示したもので、（ａ）図はマスターキーＫｍとチャネルサブキーＨの更新時期が同じ場合で、（ｂ）図はマスターキーＫｍの更新時期が例えば２ヶ月毎であるのに対し、チャネルサブキーＨの更新時期が１ヶ月毎である場合を示している。
【図２８】図２６の受信装置の処理動作を説明するためのフローチャート。
【図２９】図２６の受信装置の処理動作を説明するためのフローチャート。
【図３０】図２６の受信装置の処理動作を説明するためのフローチャート。
【図３１】本発明の第３の実施形態に係る放送受信装置の構成例を示した図。
【図３２】第３の実施形態の放送コンテンツの暗号化に用いる４段の鍵構成を説明するための図。
【図３３】通常チャネルによる配信構造の一例を示した図。
【図３４】通常チャネルにて配信される放送コンテンツ情報の構造の一例を示した図。
【図３５】通常チャネルにて配信されるチャネルキー情報の構造の一例を示した図。
【図３６】契約情報チャネルの配信構造の一例を示した図。
【図３７】契約情報チャネルにて配信される契約情報バケットの構造の一例を示した図。
【図３８】契約情報バケットに含まれる受信契約情報の構造の一例を示した図。
【図３９】契約情報チャネルにて配信されるマスター鍵シード情報の構造の一例を示した図。
【図４０】チャネルキー切替え時点でチャネルキー「０」とチャネルキー「１」の送信がオーバーラップする時間帯（Ｔｘ１、Ｔｘ２）が存在する様子を説明するための図。
【図４１】チャネルキー格納部１１１７におけるチャネルキーとその識別子との格納形態の一例を示した図。
【図４２】放送受信装置の処理動作を説明するためのフローチャート。
【図４３】放送受信装置の処理動作のうち、放送コンテンツに対する処理動作を示したフローチャート。
【図４４】放送受信装置の処理動作のうち、チャネルキー情報に対する処理動作を示したフローチャート。
【図４５】放送受信装置の処理動作のうち、契約情報バケットに対する処理動作を示したフローチャート。
【図４６】暗号化された鍵情報に対する認証子について

説明するための図。
【図４７】暗号化されない鍵情報に対する認証子について説明するための図。
【図４８】暗号化されない鍵情報に対する認証子について説明するための図。
【図４９】複数の放送受信装置の受信契約情報を圧縮して送信する場合の送信形態の一例を示した図。
【図５０】複数の放送受信装置の受信契約情報を圧縮して送信する場合の送信形態の他の例を示した図。
【図５１】本発明の第４の実施形態に係る放送受信装置の構成例を示した図。
【図５２】第４の実施形態の放送コンテンツの暗号化に用いる３段の鍵構成を説明するための図。
【図５３】通常チャネルによる配信構造の一例を示した図。
【図５４】契約情報チャネルにて配信される契約情報バケットの構造の一例を示した図。
【図５５】受信契約情報の構造の一例を示した図。
【図５６】契約情報バケットの構造の一例を示した図。
【図５７】受信契約情報の構造の他の例を示した図。
【図５８】受信契約情報の構造のさらに他の例を示した図。
【図５９】図５１のチャネルキー格納部における信契約情報にて示されたチャネル識別子とチャネルキー識別子の格納形式の一例を示した図。
【図６０】受信契約情報中にチャネルキー復号鍵が含まれる場合とチャネルキーが含まれる場合とを受信契約情報に付加された情報識別子にて区別して、処理を切り替える放送受信装置の構成例を示した図。
【図６１】本発明の第５の実施形態に係る放送受信装置の構成例を示した図。
【図６２】スキャンバステスト用第１のラッチ部の基本的な構成例を示した図。
【図６３】図６２のスキャンバステスト用第１のラッチ部の処理動作を説明するためのフローチャート。
【図６４】スキャンバス出力が可である受信契約情報を含む契約情報バケットであるか否かを判定するための認証情報を含む契約情報バケットの一例を示した図。
【図６５】図６２のスキャンバステスト用第１のラッチ部の他の処理動作を説明するためのフローチャートで、認証情報として電子署名を用いた場合を示したものである。
【図６６】スキャンバステスト用第１のラッチ部の他の構成例を示した図で、出力する内部データ（受信契約情報）を暗号化して出力するための構成部を追加したものである。
【図６７】スキャンバステスト用第２のラッチ部の構成例を示した図。
【図６８】受信契約情報にデジタル署名が含まれる場合の放送受信装置の認証部１１１４の構成例を示した図。
【図６９】デジタル署名が含まれている場合の受信契約情報の構造例を示した図。
【図７０】第３の実施形態に係る契約管理装置の構成例を示した図。
【図７１】第４の実施形態に係る契約管理装置の構成例を示した図。
【図７２】契約管理装置の契約情報バケット生成部の構成例を示した図。
【図７３】契約情報バケット生成部の処理動作を説明するためのフローチャート。
【図７４】第３の実施形態で用いる受信契約情報の基本的な構成例を示した図。
【図７５】復号の際の誤り検出に用いる認証子を含む受信契約情報の構成を示した図。
【図７６】復号の際の誤り検出に用いる認証子とデジタル署名とを含む受信契約情報の構成を示した図。
【図７７】受信契約情報に認証子とデジタル署名を含む場合の契約情報バケットの送信形態の一例を示した図。
【図７８】受信契約情報に認証子とデジタル署名を含む場合の契約情報バケットの送信形態の他の例を示した図。
【図７９】第４の実施形態に係る複数の放送受信装置の受信契約情報（チャネルキーが２つある場合）を圧縮して送信する場合の送信形態の一例を示した図。
【図８０】第４の実施形態に係る複数の放送受信装置の受信契約情報（チャネルキーが２つある場合）を圧縮して送信する場合の送信形態の他の例を示した図。
【図８１】カードに受信契約情報を書き込んで配布する契約管理装置の構成例を示した図。
【図８２】配布されたカードから受信契約情報を読み取る放送受信装置の構成例を示した図。
【符号の説明】
契約管理装置
１…契約ユーザデータベース
２…支払い確認待ちデータベース
３…シードデータベース
４…チャネルキーデータベース
５…付加情報データベース
６…契約解除ユーザデータベース
７…契約期間確認部
８…付加情報生成部
９…付加情報生成制御部
１０…シード・マスターキー生成部
１１…チャネルキー生成部
１２…付加情報出力要請部
１３…放送装置
１４…スケジューリング部
１５…カード作成部
２００８…契約情報バケット生成部
２００９…契約情報バケット生成制御部

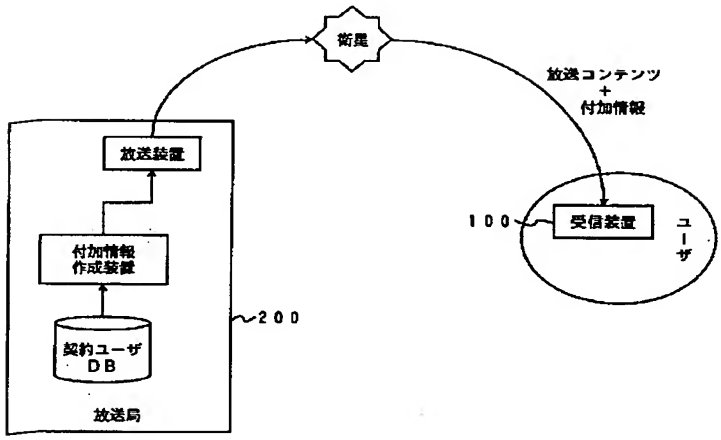
63

２０５１…カード作成部
放送受信装置
５０１…受信部
５０２…Ａ／Ｄ変換部
５０３…フィルタ
５０４…マスターキー生成部
５０５…マスターキー格納部
５０６…ＩＤ格納部
５０７…判定部
５０８…チャネルサブキー格納部
５０９…チャネルデコーダ
５１０…Ｄ／Ａ変換部
５１１…再生部
５１２…付加情報格納部

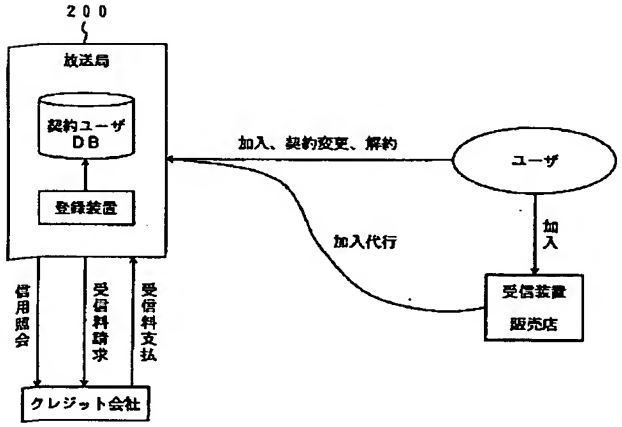
64

＊５１３…カードリーダ
１１０６…課金制御部
１１０９…チャネルキー復号部
１１１０…契約情報復号部
１１１１…マスター鍵格納部
１１１４…認証部
１１１８…契約判定部
１１２０…チャネルキー出力部
１２０１…スキャンバステスト用第１のラッチ部
１２０２…第１のスキャンバス出力部
１２０３…スキャンバステスト用第２のラッチ部
１２０４…第２のスキャンバス出力部
２０６１…カードリーダ
＊

【図１】



【図２】



【図４】

契約ユーザＤＢ

受信端末ＩＤ	チャネル番号	契約期間

【図６】

チャネルキーＤＢ

チャネル番号	チャネルキーＩＤ	チャネルキー	有効期間

【図４１】

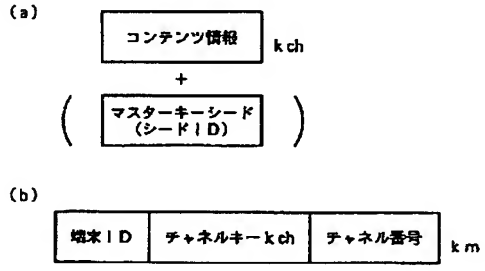
チャネルキー	0
チャネルキー	1

【図５】

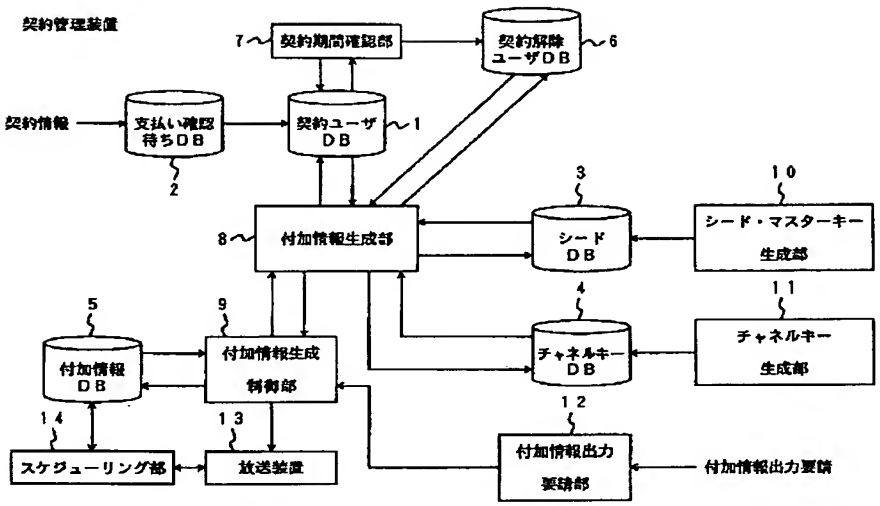
シードＤＢ

シードＩＤ	マスターキー	有効期間

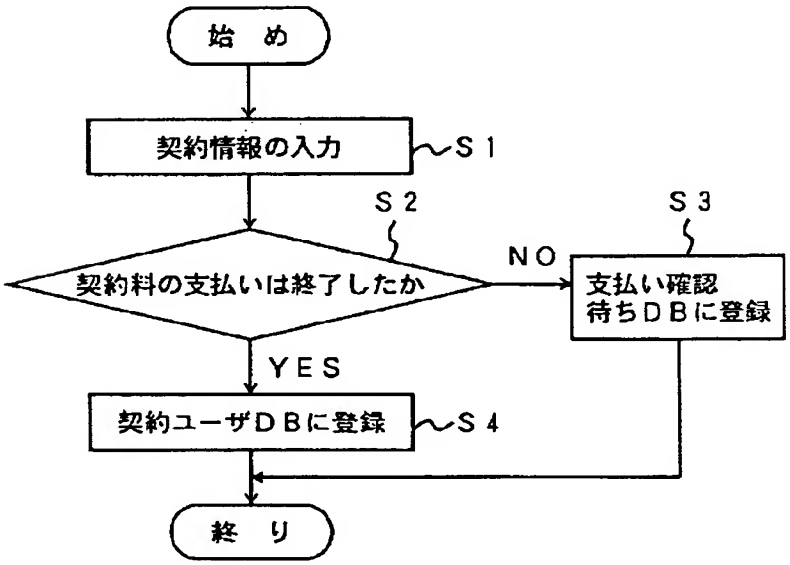
【図９】



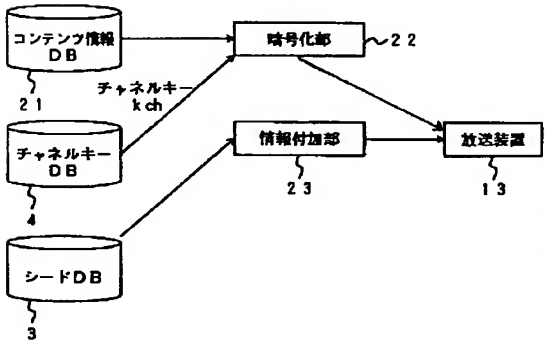
【図３】



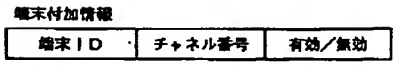
【図７】



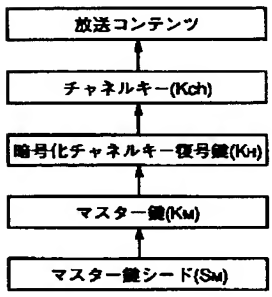
【図１０】



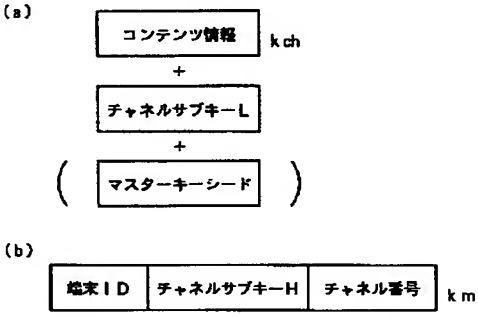
【図１２】



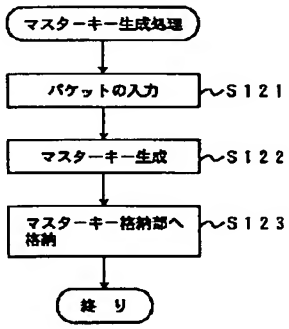
【図３２】



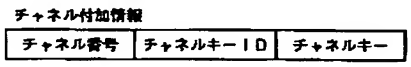
【図１１】



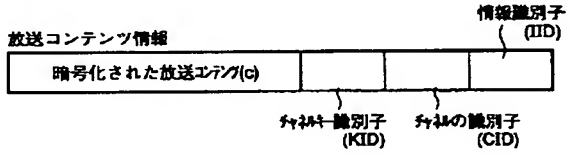
【図１６】



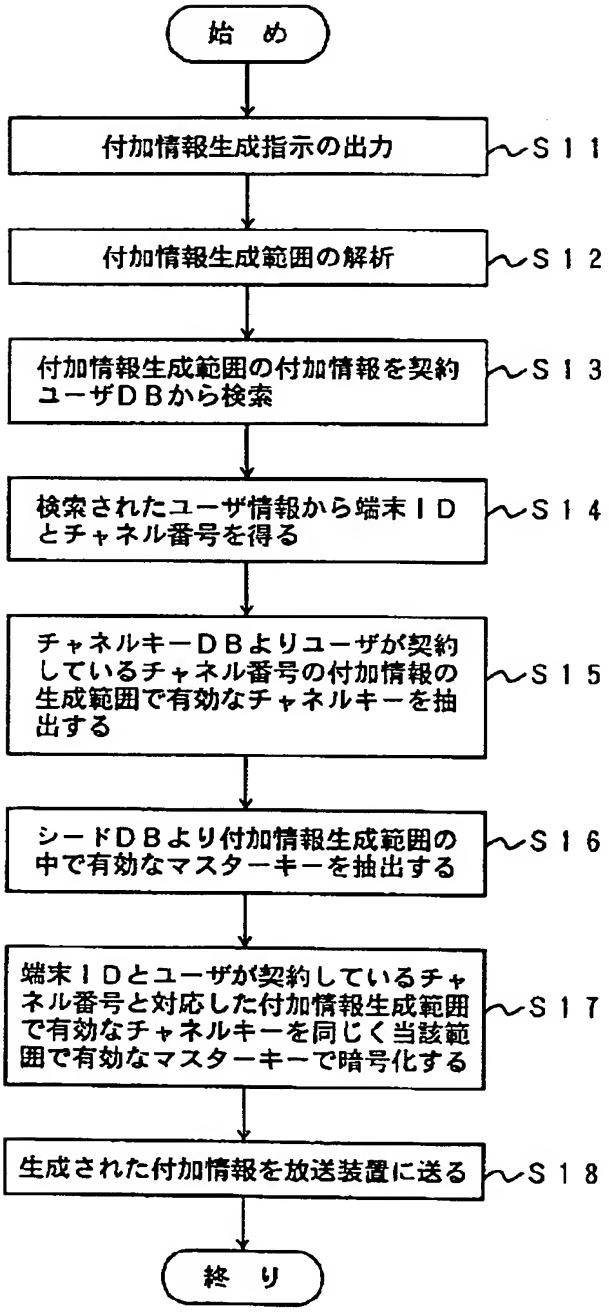
【図１３】



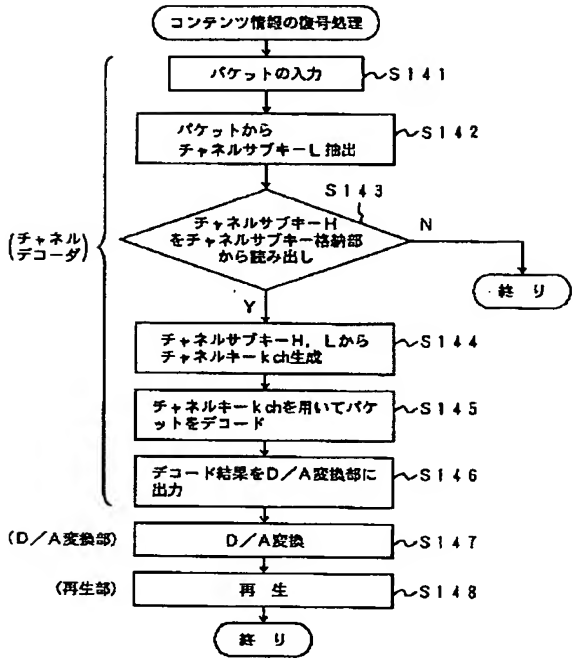
【図３４】



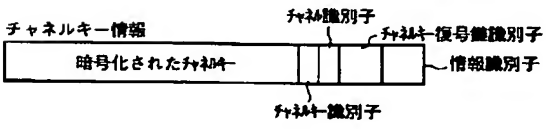
【図８】


始　め
付加情報生成指示の出力
S１１
付加情報生成範囲の解析
S１２
付加情報生成範囲の付加情報を契約ユーザＤＢから検索
S１３
検索されたユーザ情報から端末ＩＤとチャネル番号を得る
S１４
チャネルキーＤＢよりユーザが契約しているチャネル番号の付加情報の生成範囲で有効なチャネルキーを抽出する
S１５
シードＤＢより付加情報生成範囲の中で有効なマスターキーを抽出する
S１６
端末ＩＤとユーザが契約しているチャネル番号と対応した付加情報生成範囲で有効なチャネルキーを同じく当該範囲で有効なマスターキーで暗号化する
S１７
生成された付加情報を放送装置に送る
S１８
終　り

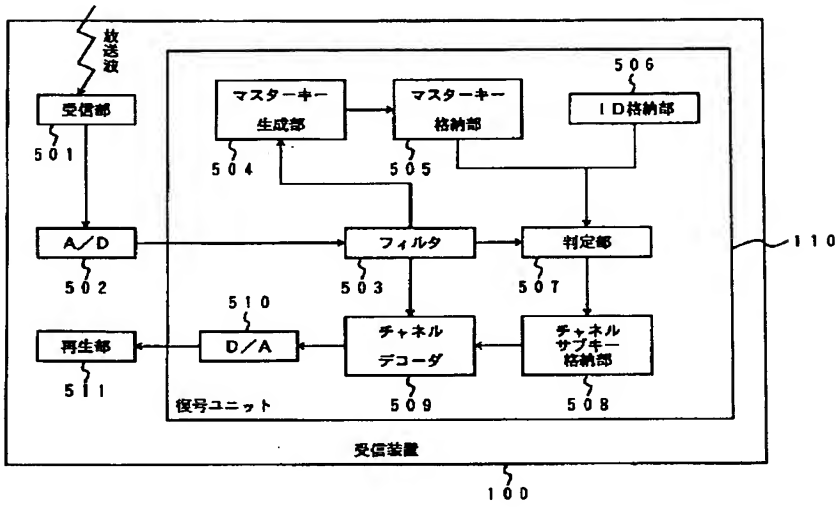
【図１８】


コンテンツ情報の復号処理
パケットの入力
S１４１
パケットから
チャネルサブキーＬ抽出
S１４２
S１４３
チャネルサブキーＨ
をチャネルサブキー格納部
から読み出し
N
Y
終　り
(チャネル)
(デコーダ)
チャネルサブキーＨ，Ｌから
チャネルキーｋch生成
S１４４
チャネルキーｋchを用いてパケットをデコード
S１４５
デコード結果をＤ／Ａ変換部に出力
S１４６
(Ｄ／Ａ変換部)
Ｄ／Ａ変換
S１４７
(再生部)
再　生
S１４８
終　り

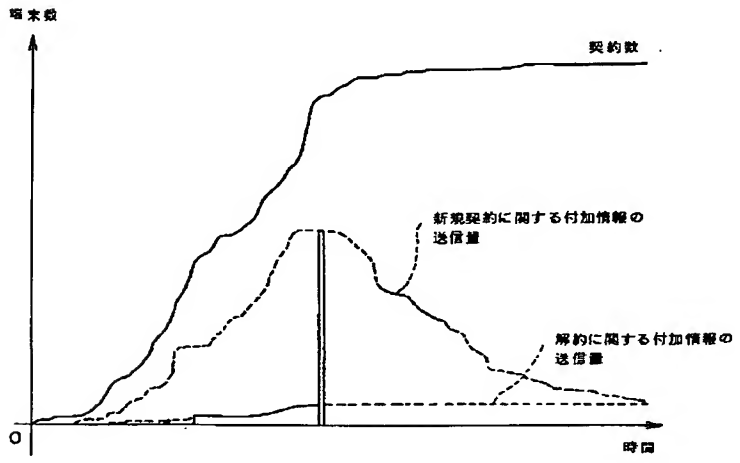
【図３５】


チャネルキー情報
チャネル識別子
チャネルキー復号鍵識別子
暗号化されたチャネルキー
情報識別子
チャネルキー識別子

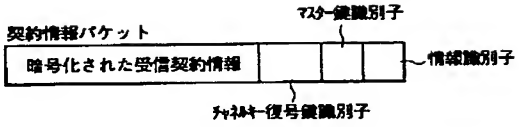
【図１４】



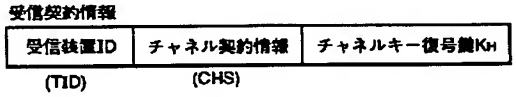
【図１９】



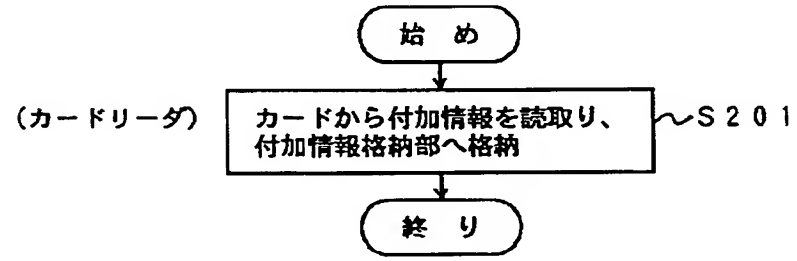
【図３７】



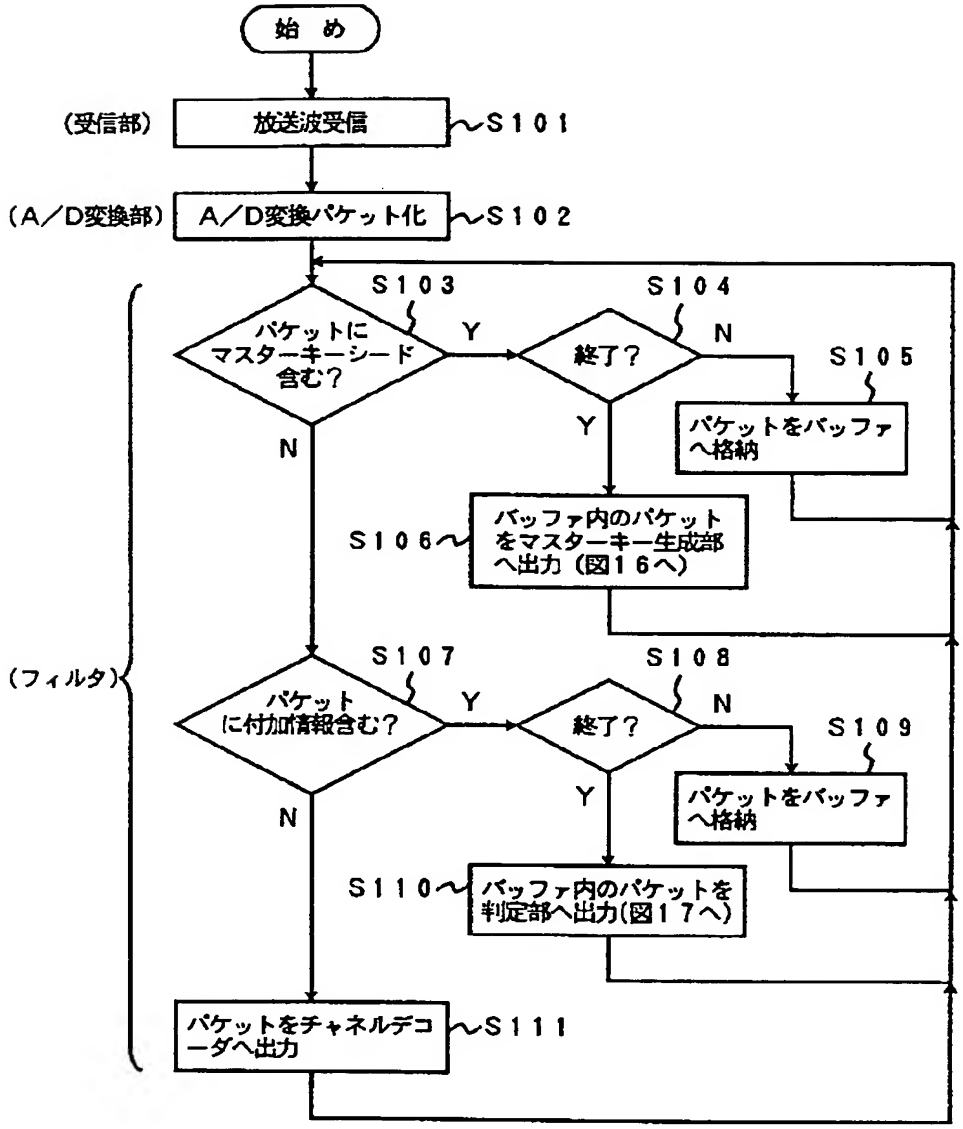
【図３８】



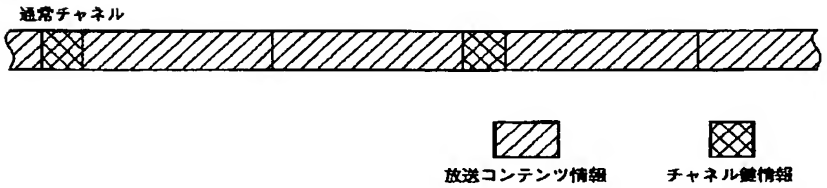
【図２８】



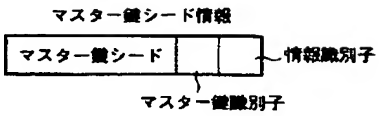
【図１５】


始　め
(受信部)
放送波受信
S１０１
(A／D変換部)
A／D変換パケット化
S１０２
S１０３
パケットに
マスターキーシード
含む?
Y
S１０４
終了?
N
S１０５
パケットをバッファ
へ格納
Y
N
S１０６
バッファ内のパケット
をマスターキー生成部
へ出力（図１６へ）
(フィルタ)
S１０７
パケット
に付加情報含む?
Y
S１０８
終了?
N
S１０９
パケットをバッファ
へ格納
Y
N
S１１０
バッファ内のパケットを
判定部へ出力(図１７へ)
パケットをチャネルデコ
ーダへ出力
S１１１

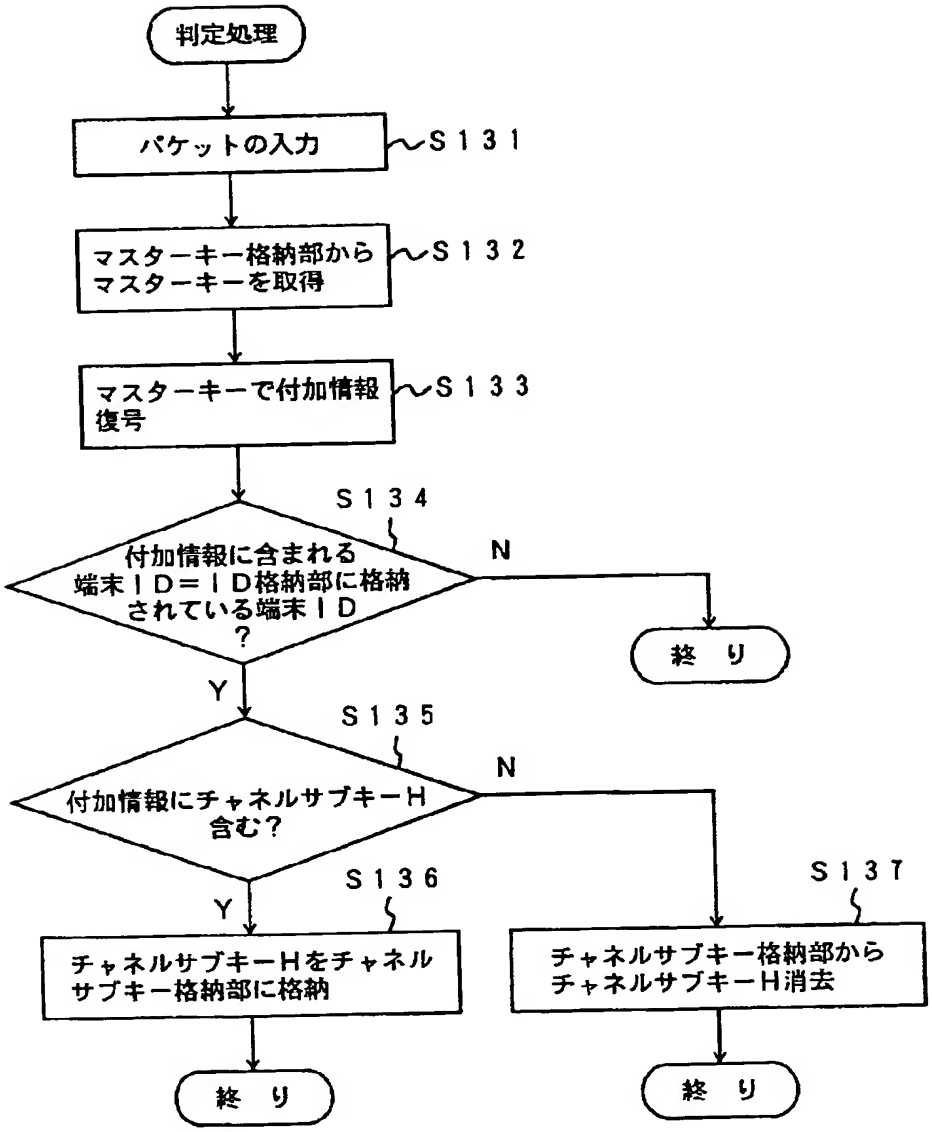
【図３３】


通常チャネル
放送コンテンツ情報
チャネル鍵情報

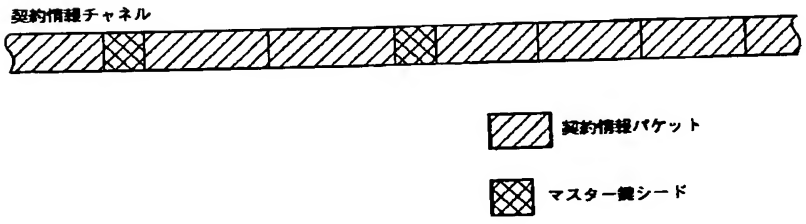
【図３９】


マスター鍵シード情報
マスター鍵シード
情報識別子
マスター鍵識別子

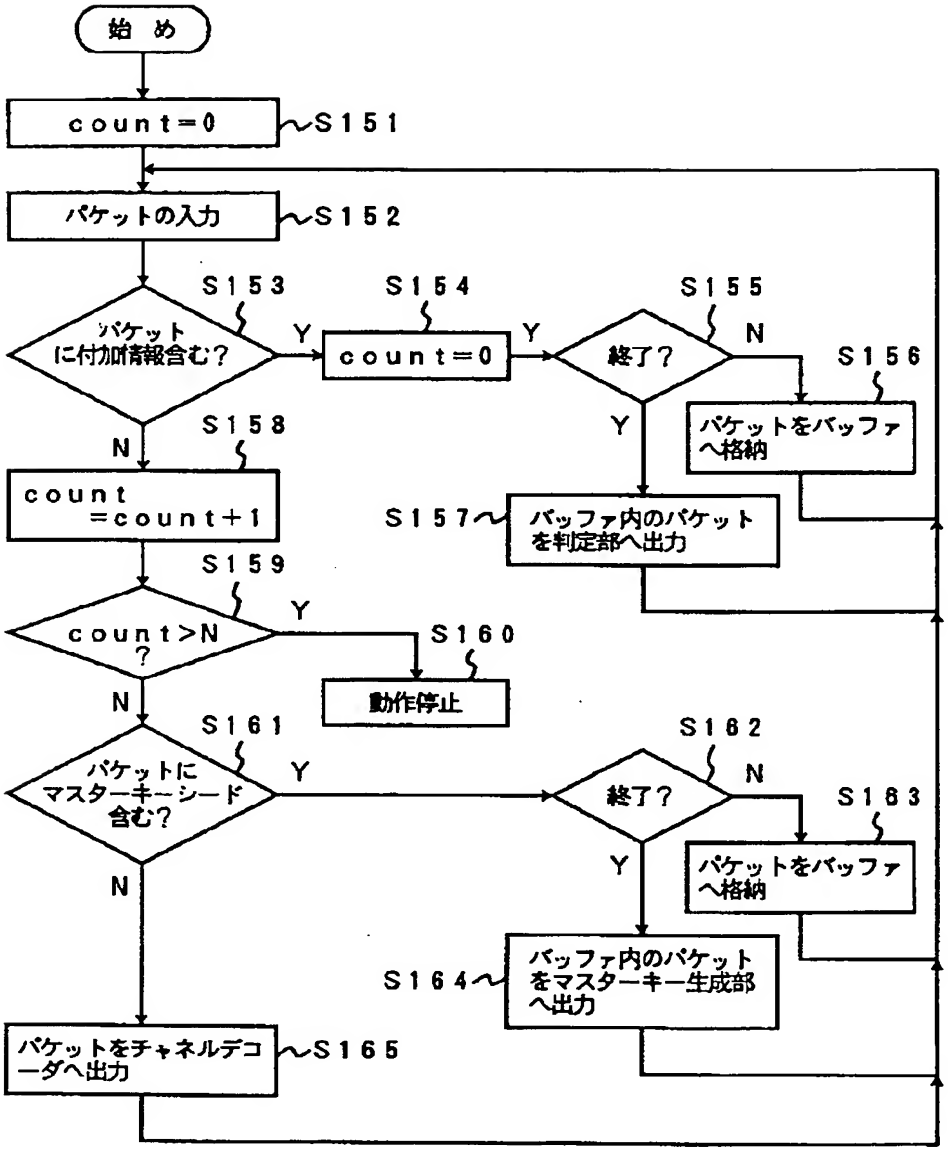
【図１７】


判定処理
パケットの入力
S１３１
マスターキー格納部から
マスターキーを取得
S１３２
マスターキーで付加情報
復号
S１３３
S１３４
付加情報に含まれる
端末ＩＤ＝ＩＤ格納部に格納
されている端末ＩＤ
？
N
終　り
Y
S１３５
付加情報にチャネルサブキーＨ
含む？
N
Y
S１３６
チャネルサブキーＨをチャネル
サブキー格納部に格納
終　り
S１３７
チャネルサブキー格納部から
チャネルサブキーＨ消去
終　り

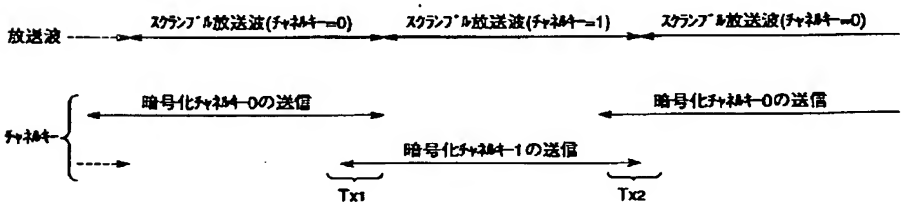
【図３６】


契約情報チャネル
契約情報パケット
マスター鍵シード

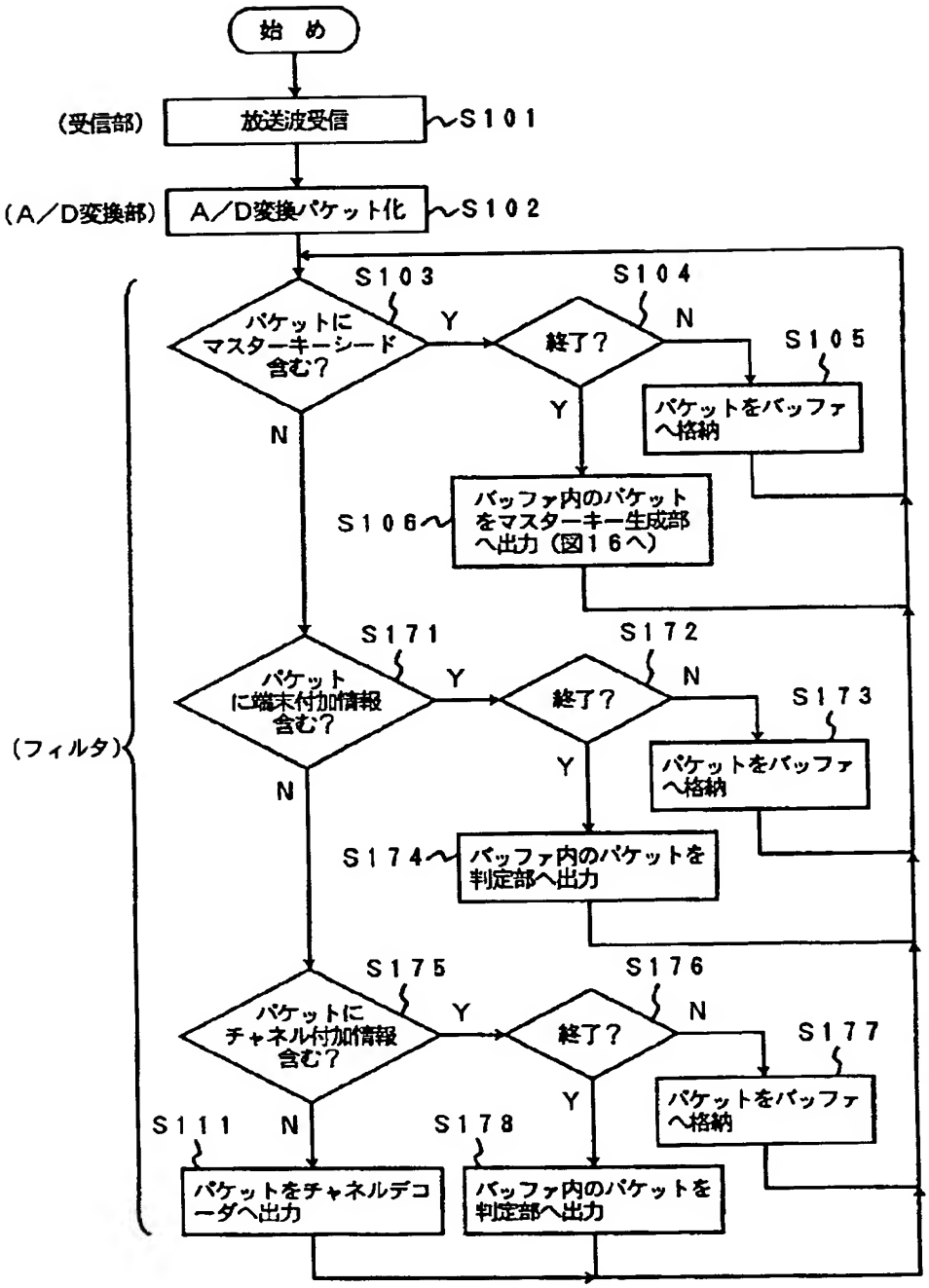
【図２０】


始め
count＝0
S151
パケットの入力
S152
S153
パケットに付加情報含む？
Y
S154
count＝0
Y
S155
終了？
N
S156
パケットをバッファへ格納
Y
N
S158
count＝count＋1
S157
バッファ内のパケットを判定部へ出力
S159
count＞N？
Y
S160
動作停止
N
S161
パケットにマスターキーシード含む？
Y
S162
終了？
N
S163
パケットをバッファへ格納
Y
N
S164
バッファ内のパケットをマスターキー生成部へ出力
パケットをチャネルデコーダへ出力
S165

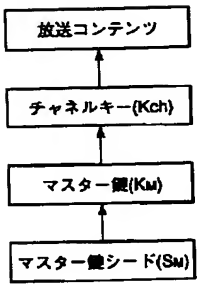
【図４０】


放送波
スクランブル放送波(チャネルキー=0)
スクランブル放送波(チャネルキー=1)
スクランブル放送波(チャネルキー=0)
チャネルキー
暗号化チャネルキー0の送信
暗号化チャネルキー0の送信
暗号化チャネルキー1の送信
Tx1
Tx2

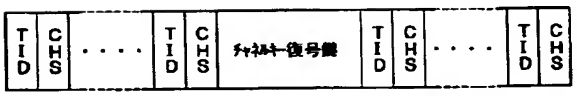
【図２１】



【図５２】

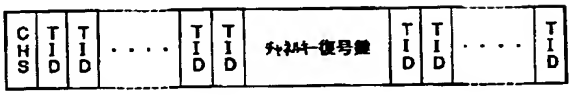


【図４９】

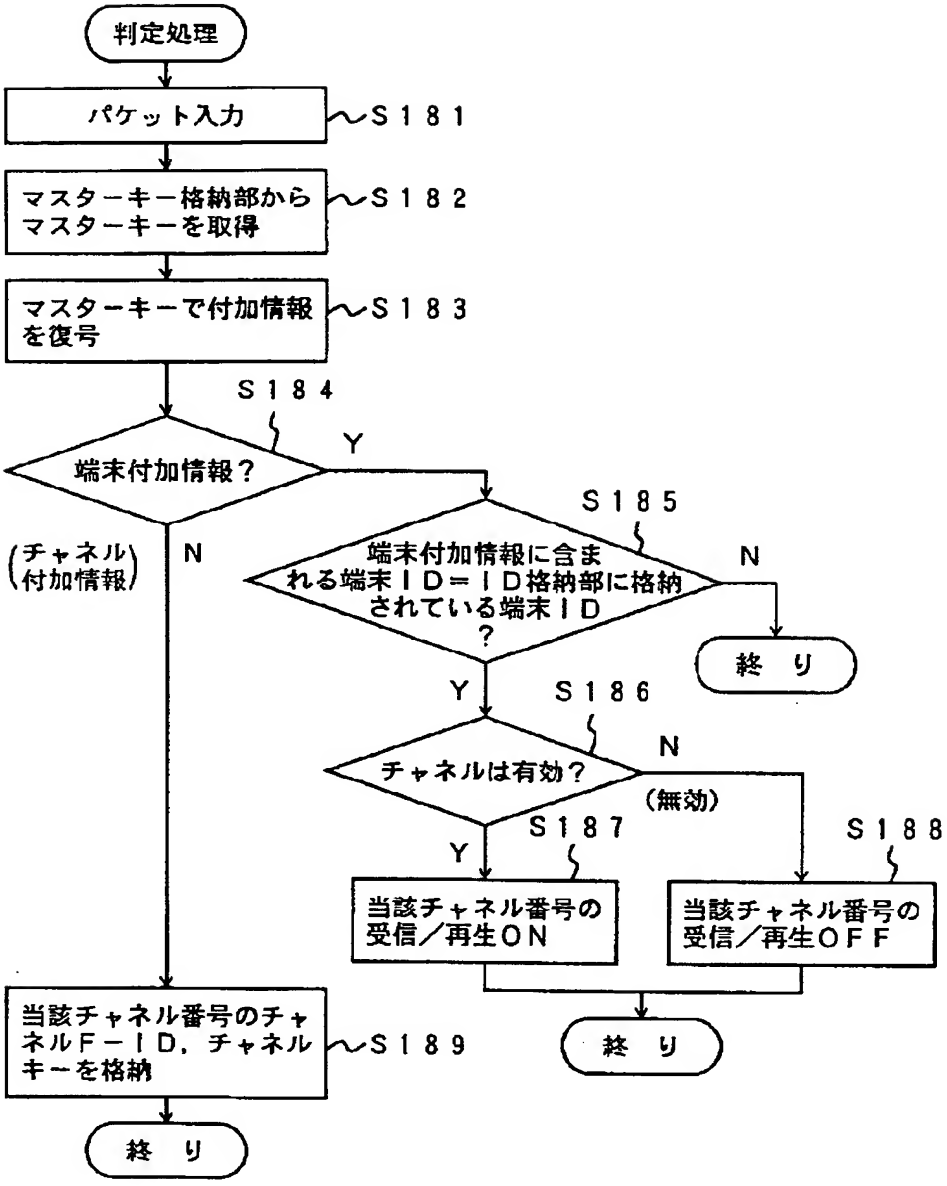


TID：受信装置ID
CHS：チャネル契約情報

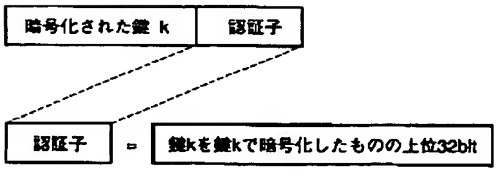
【図５０】



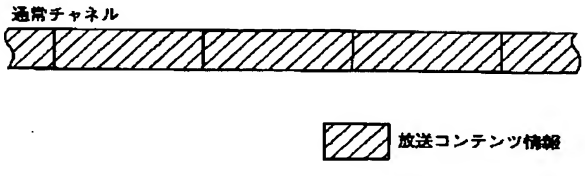
【図２２】


判定処理
パケット入力
S１８１
マスターキー格納部から
マスターキーを取得
S１８２
マスターキーで付加情報
を復号
S１８３
S１８４
端末付加情報？
Y
N
(チャネル
付加情報)
S１８５
端末付加情報に含ま
れる端末ＩＤ＝ＩＤ格納部に格納
されている端末ＩＤ
？
N
終　り
Y
S１８６
チャネルは有効？
N
(無効)
Y
S１８７
S１８８
当該チャネル番号の
受信／再生ＯＮ
当該チャネル番号の
受信／再生ＯＦＦ
終　り
当該チャネル番号のチャ
ネルＦ－ＩＤ，チャネル
キーを格納
S１８９
終　り

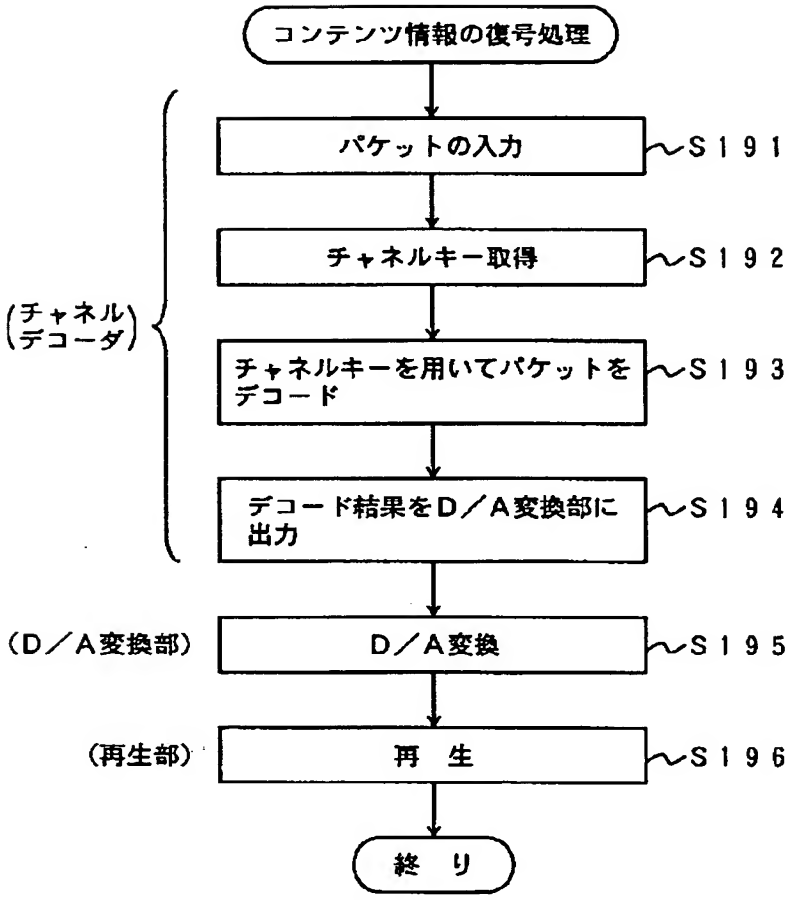
【図４６】


暗号化された鍵 k
認証子
認証子
=
鍵kを鍵kで暗号化したものの上位32bit

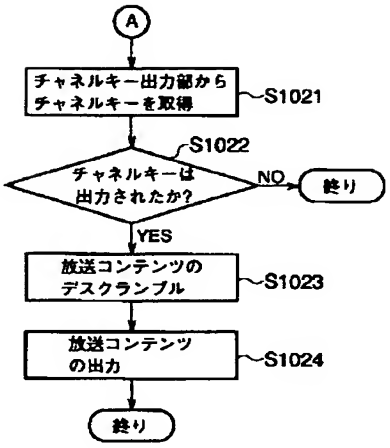
【図５３】


通常チャネル
放送コンテンツ情報

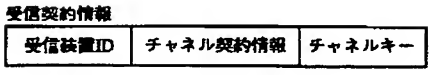
【図２３】



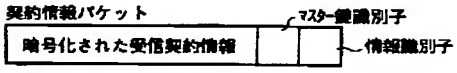
【図４３】



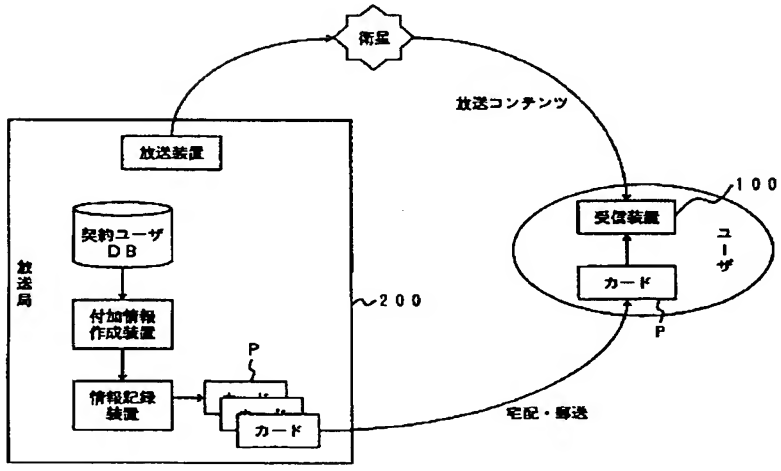
【図５５】



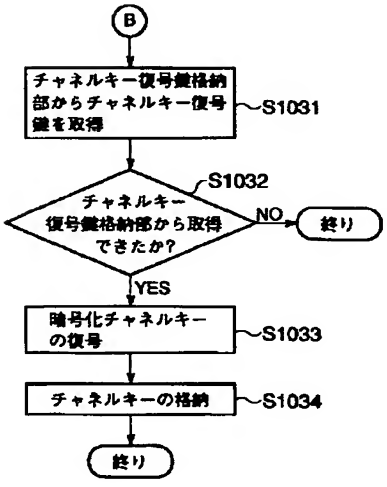
【図５６】



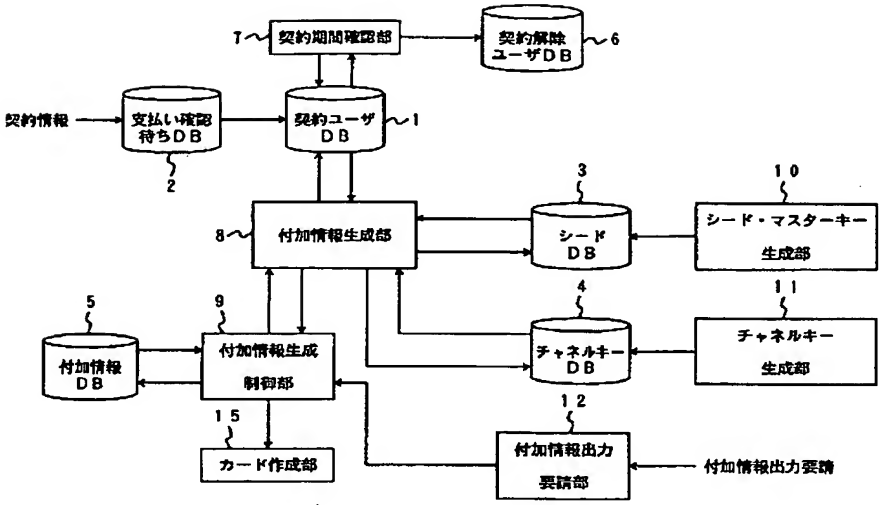
【図２４】



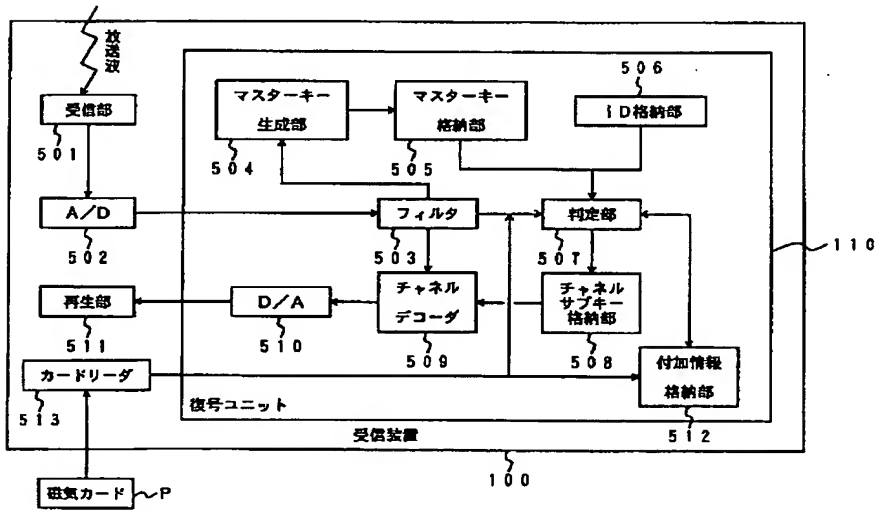
【図４４】



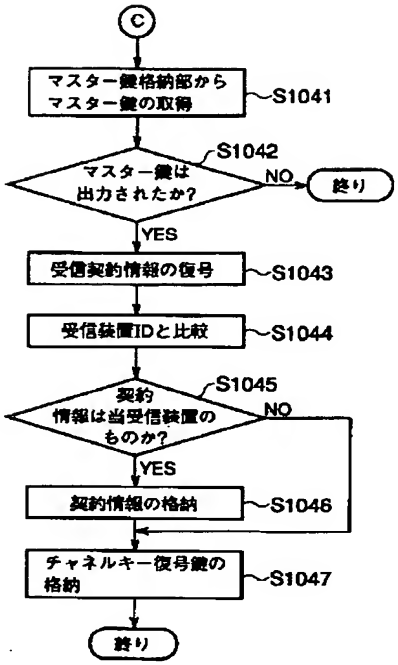
【図２５】



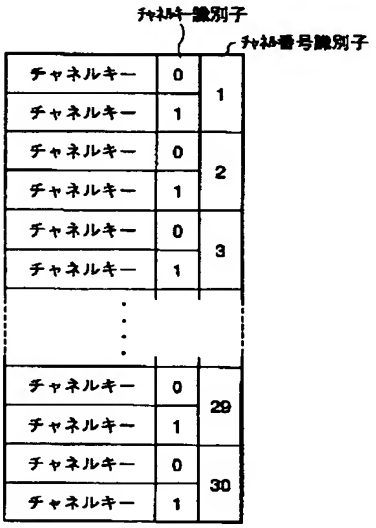
【図２６】



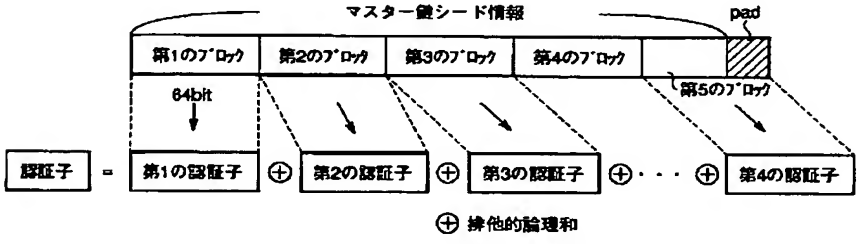
【図４５】



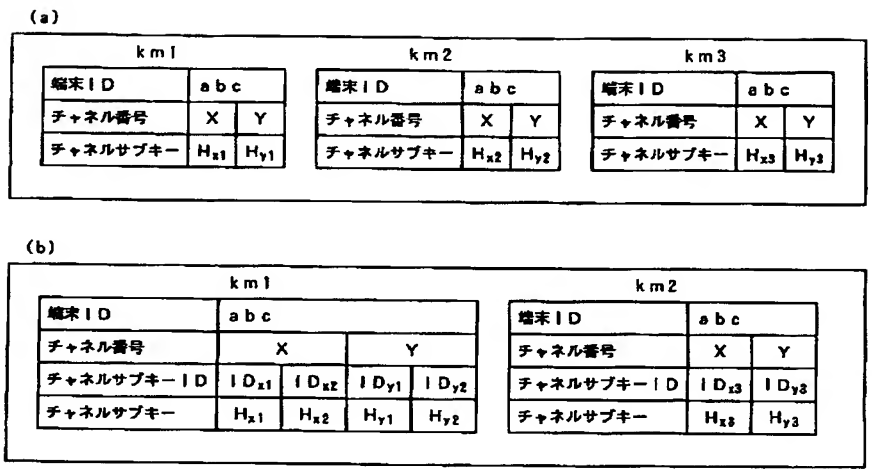
【図５９】



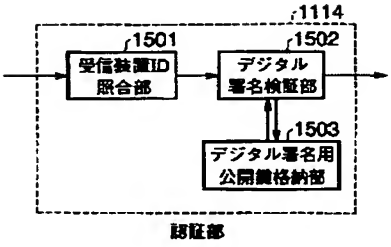
【図４７】



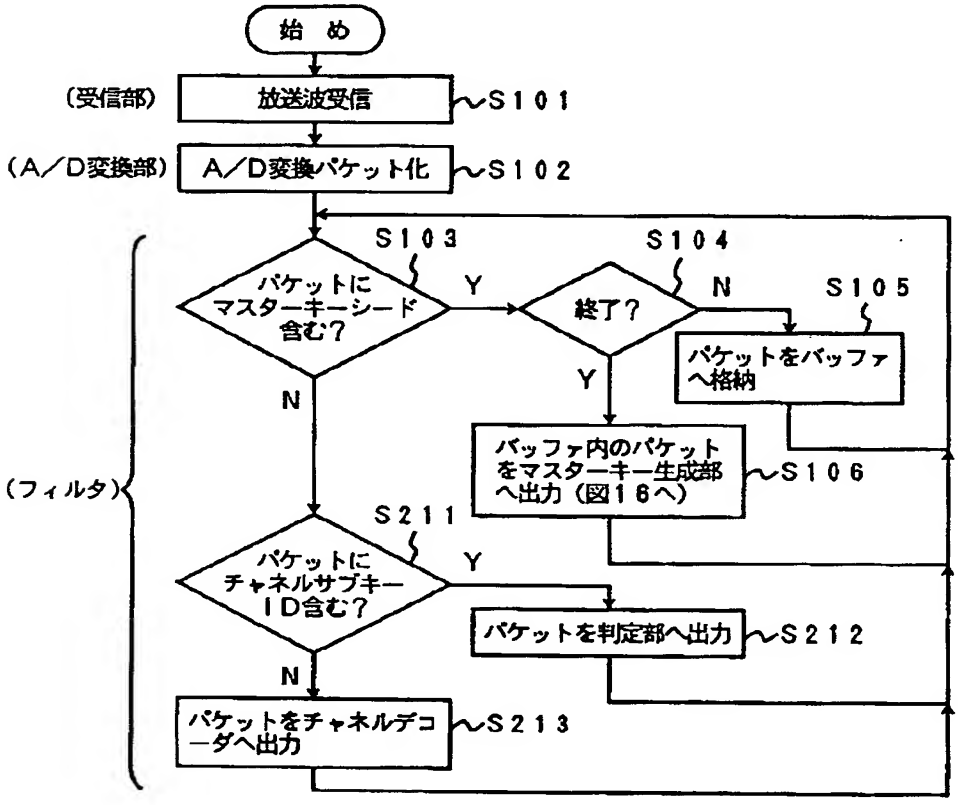
【図２７】



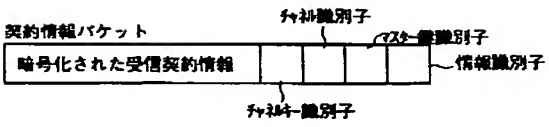
【図６８】



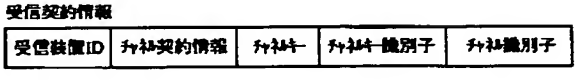
【図２９】



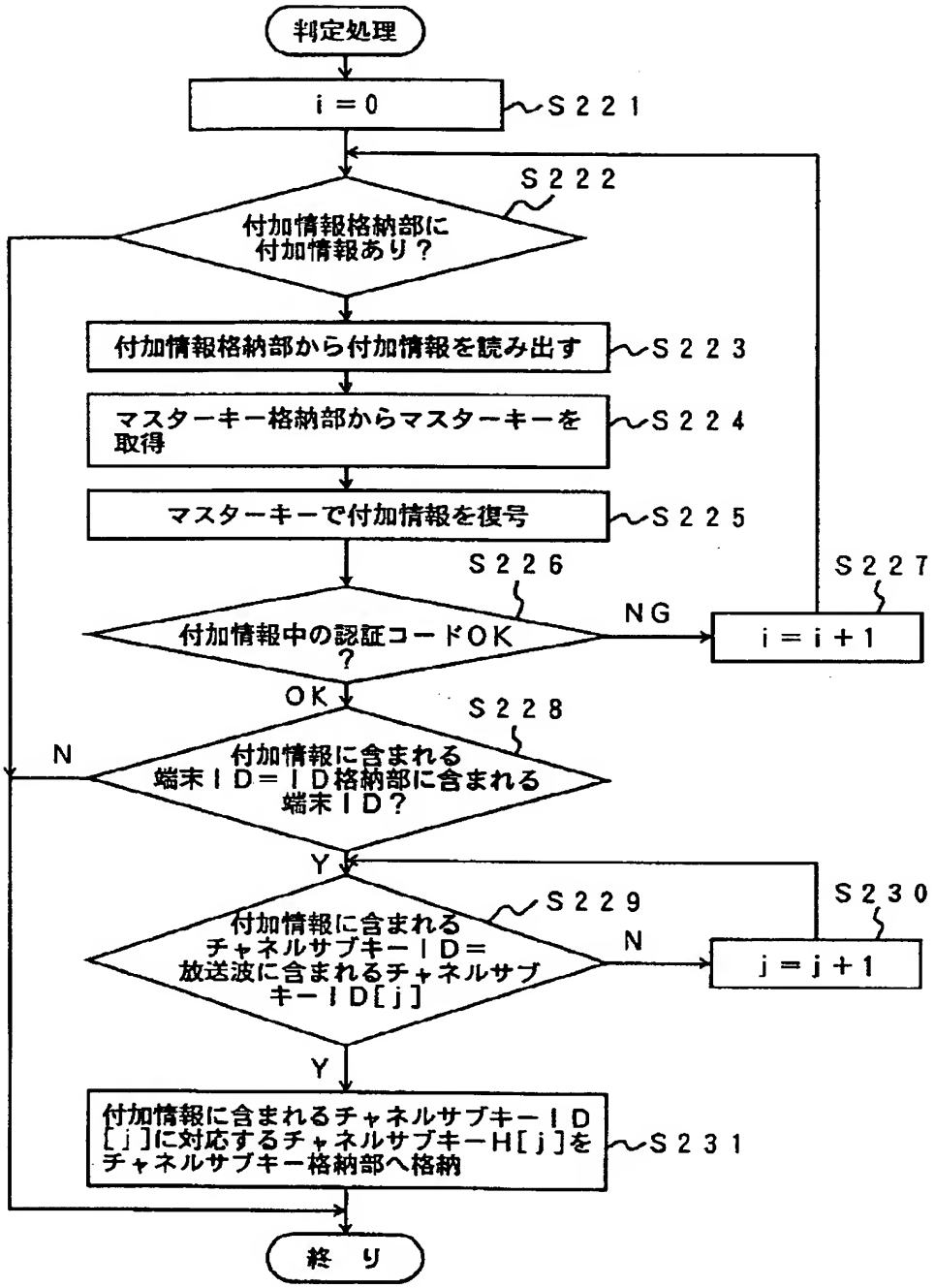
【図５４】



【図５７】



【図３０】



【図５８】

受信契約情報

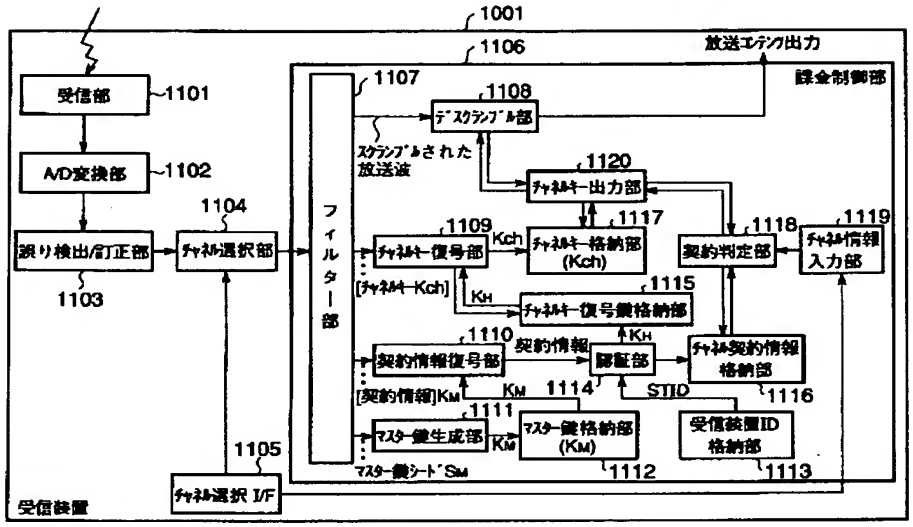
受信装置ID	チャネル契約情報	チャネルキー0	チャネルキー1	チャネル識別子

【図６４】

契約情報パケット

暗号化された受信契約情報	認証情報	チャネルキー復号鍵識別子	マスター鍵識別子	情報識別子

【図３１】

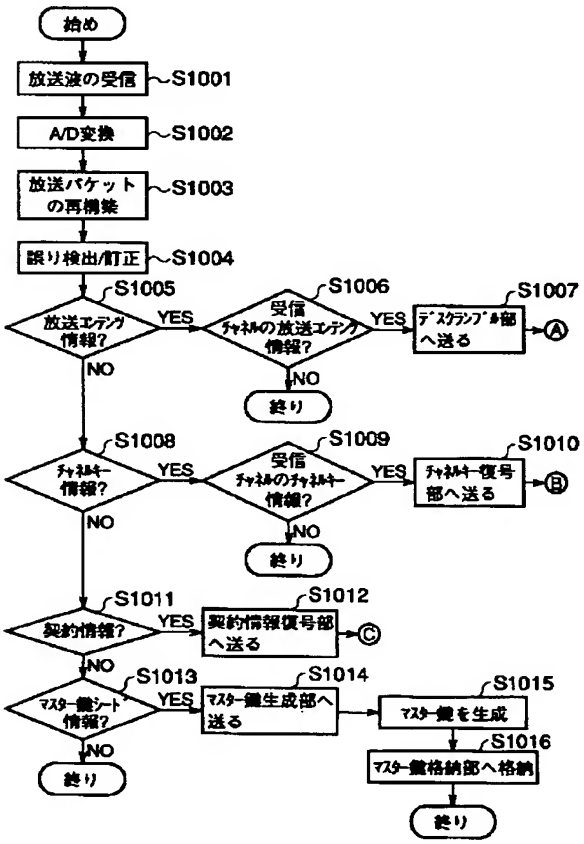


【図７４】

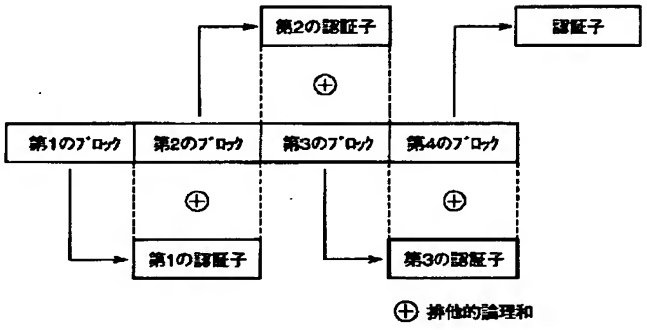
受信契約情報

受信端末ID	チャネル契約情報	チャネルキー復号鍵

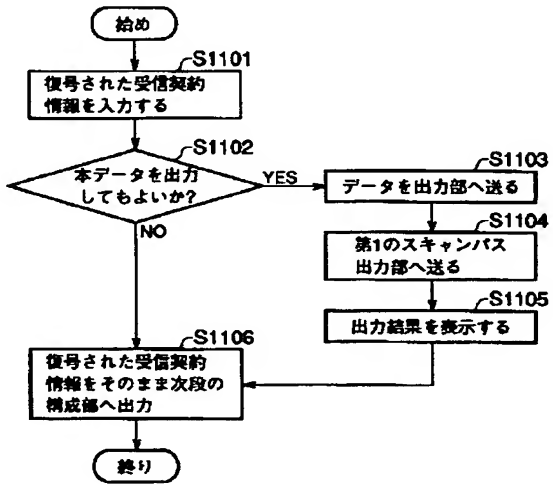
【図４２】



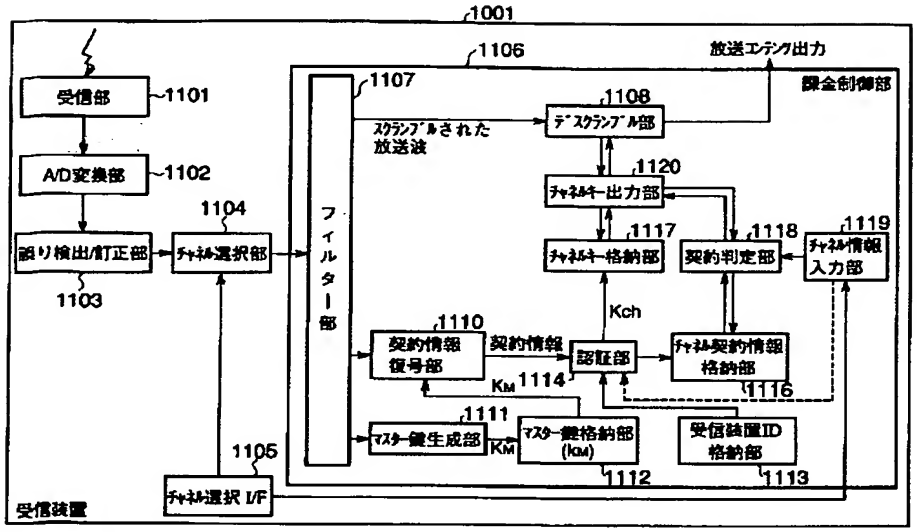
【図４８】



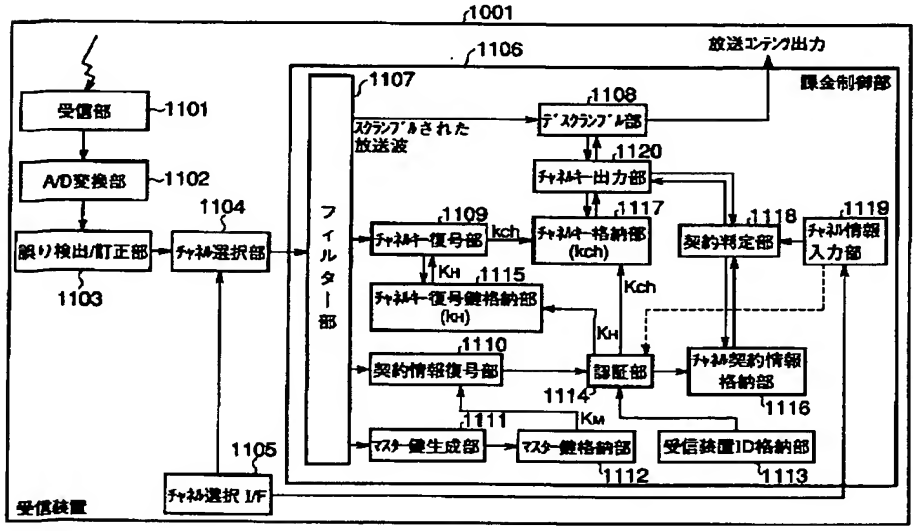
【図６３】



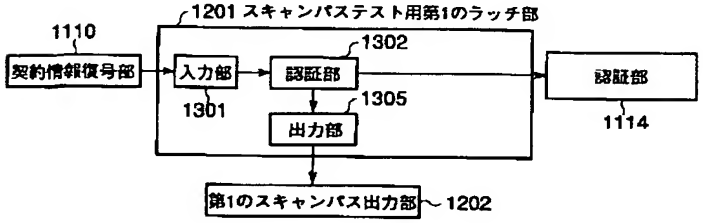
【図５１】



【図６０】



【図６２】



【図６９】

受信契約情報

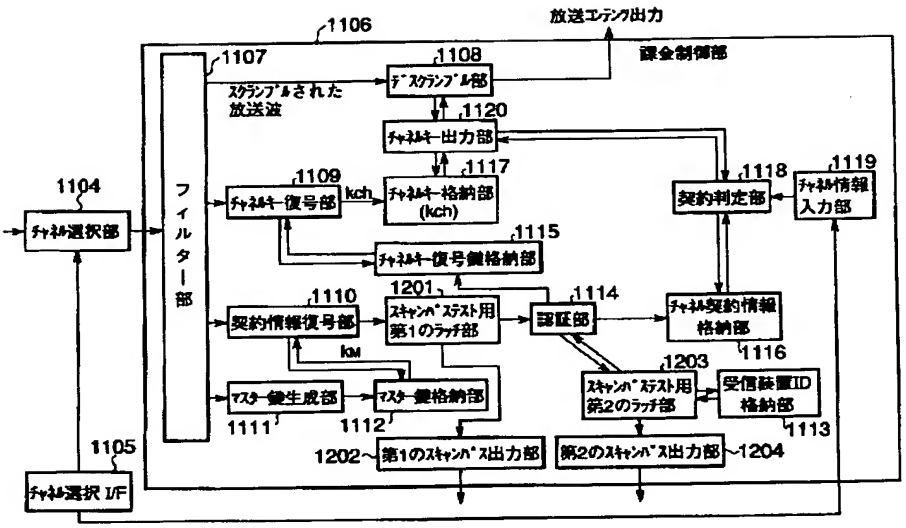
受信端末ID	チャネル契約情報	チャネルキー復号鍵	デジタル署名

【図７５】

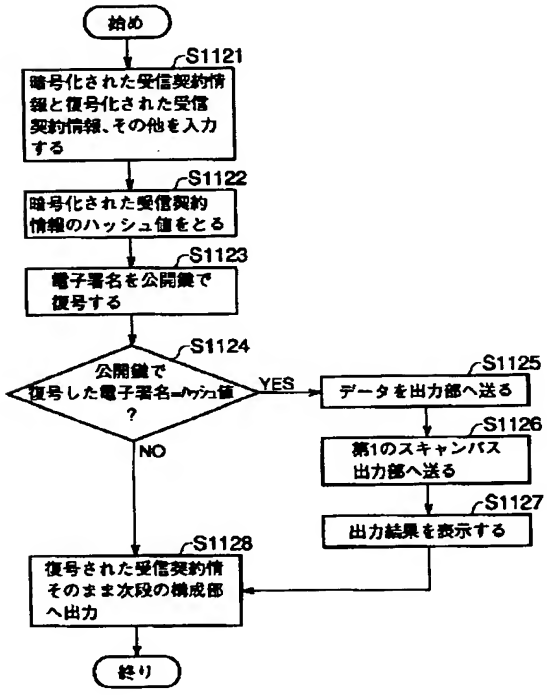
受信契約情報

受信端末ID	チャネル契約情報	チャネルキー復号鍵	認証子

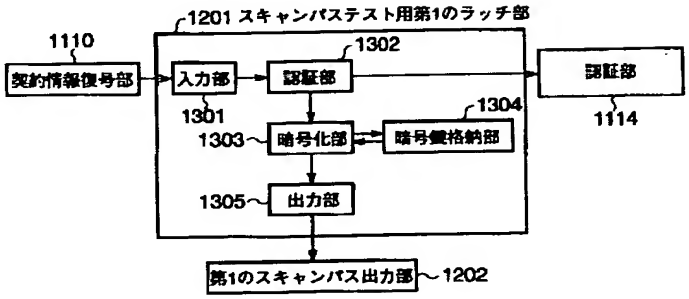
【図６１】



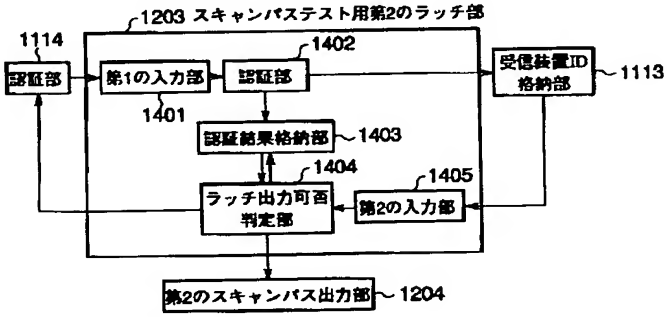
【図６５】



【図６６】



【図６７】

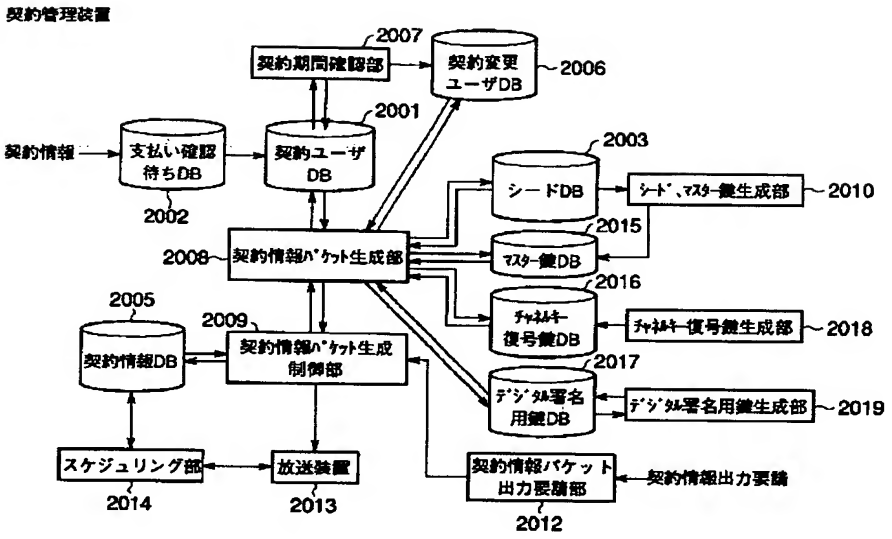


【図７６】

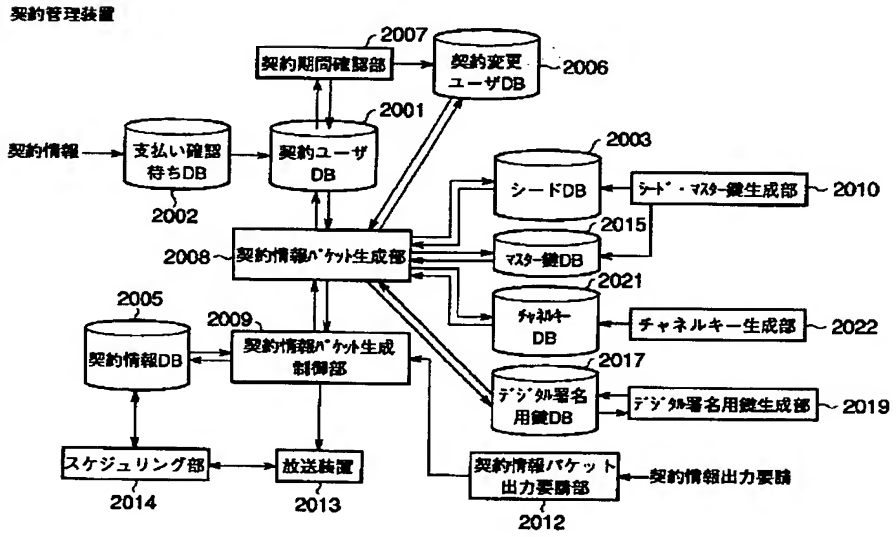
受信契約情報

受信端末ID	チャネル契約情報	チャネルキー復号鍵	認証子	デジタル署名

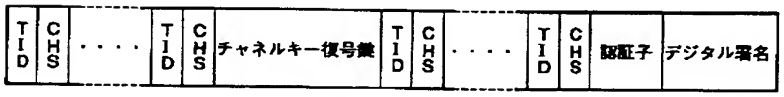
【図７０】



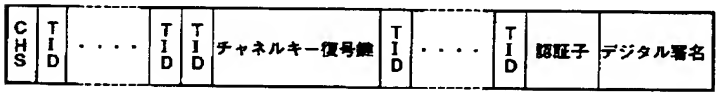
【図７１】



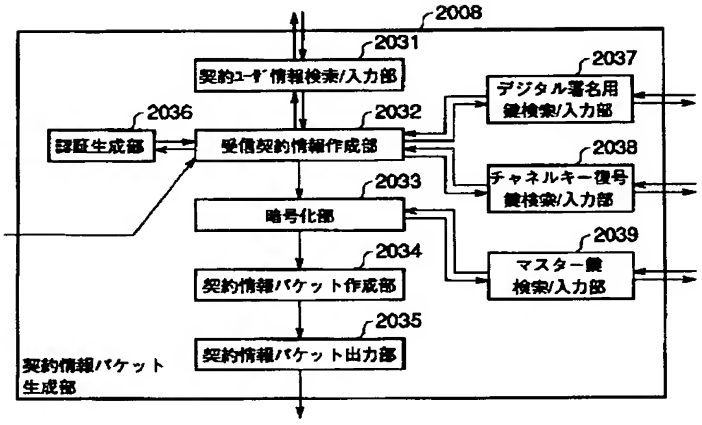
【図７７】



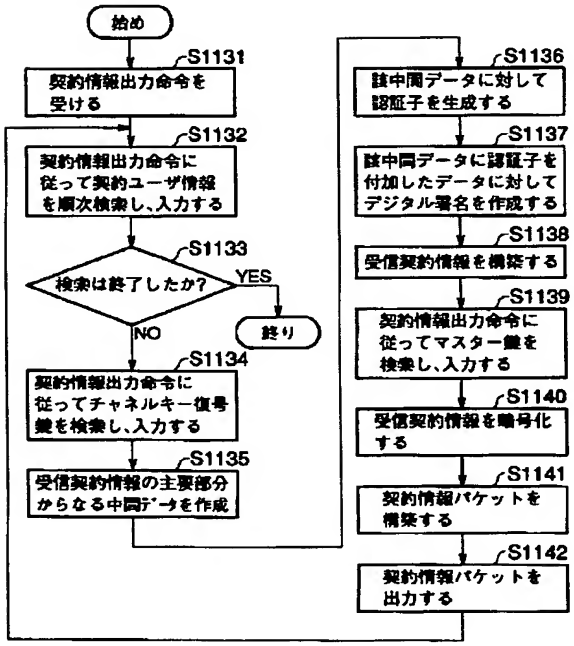
【図７８】



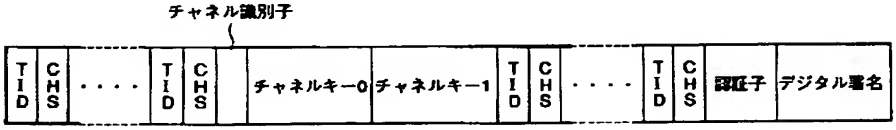
【図７２】


2008
2031
契約ユーザ情報検索/入力部
2037
デジタル署名用鍵検索/入力部
2036
認証生成部
2032
受信契約情報作成部
2038
チャネルキー復号鍵検索/入力部
2033
暗号化部
2039
マスター鍵検索/入力部
2034
契約情報パケット作成部
2035
契約情報パケット出力部
契約情報パケット生成部

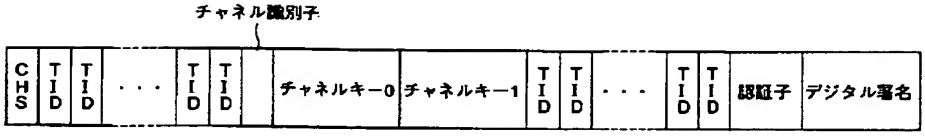
【図７３】


始め
S1131
契約情報出力命令を受ける
S1132
契約情報出力命令に従って契約ユーザ情報を順次検索し、入力する
S1133
検索は終了したか?
YES
NO
終り
S1134
契約情報出力命令に従ってチャネルキー復号鍵を検索し、入力する
S1135
受信契約情報の主要部分からなる中間データを作成
S1136
該中間データに対して認証子を生成する
S1137
該中間データに認証子を付加したデータに対してデジタル署名を作成する
S1138
受信契約情報を構築する
S1139
契約情報出力命令に従ってマスター鍵を検索し、入力する
S1140
受信契約情報を暗号化する
S1141
契約情報パケットを構築する
S1142
契約情報パケットを出力する

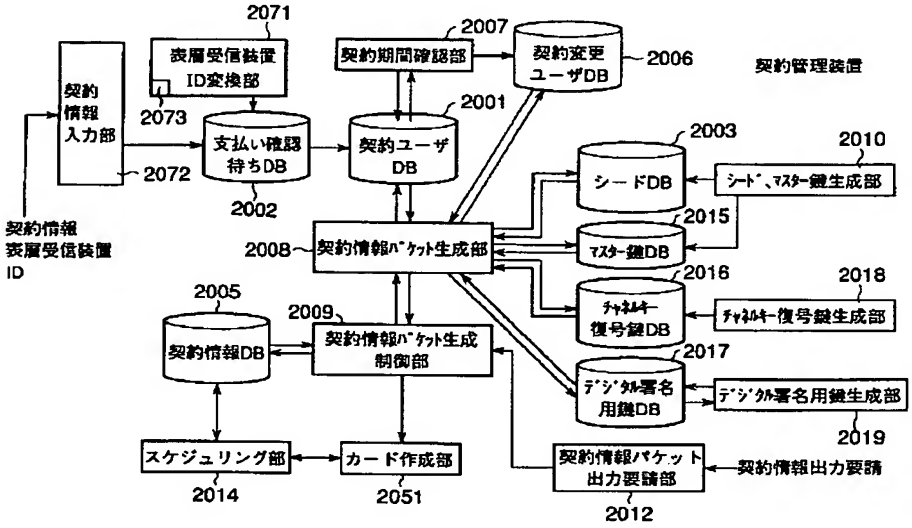
【図７９】


チャネル識別子
TID
CHS
・・・・
TID
CHS
チャネルキー0
チャネルキー1
TID
CHS
・・・・
TID
CHS
認証子
デジタル署名

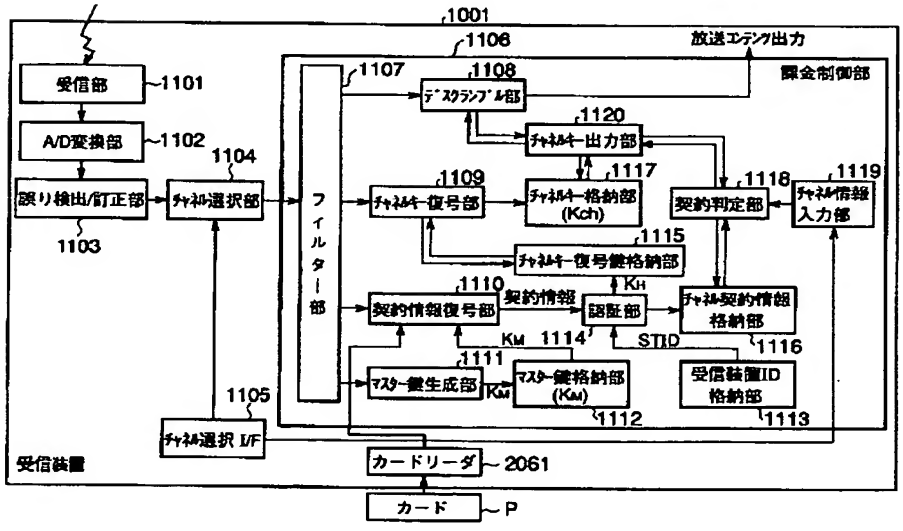
【図８０】


チャネル識別子
CHS
TID
TID
・・・
TID
TID
チャネルキー0
チャネルキー1
TID
TID
・・・
TID
TID
認証子
デジタル署名

【図８１】


2071
表層受信装置 ID変換部
2073
契約情報入力部
2072
契約情報 表層受信装置 ID
支払い確認待ちDB
2002
契約期間確認部
2007
契約変更ユーザDB
2006
契約管理装置
契約ユーザDB
2001
2008
契約情報ﾊﾟｹｯﾄ生成部
2005
契約情報DB
2009
契約情報ﾊﾟｹｯﾄ生成制御部
スケジュリング部
2014
カード作成部
2051
シードDB
2003
ｼｰﾄﾞ、ﾏｽﾀｰ鍵生成部
2010
ﾏｽﾀｰ鍵DB
2015
ﾁｬﾈﾙｷｰ復号鍵DB
2016
ﾁｬﾈﾙｷｰ復号鍵生成部
2018
ﾃﾞｼﾞﾀﾙ署名用鍵DB
2017
ﾃﾞｼﾞﾀﾙ署名用鍵生成部
2019
契約情報パケット出力要請部
2012
契約情報出力要請

【図８２】


1001
1106
放送コンテンツ出力
課金制御部
受信部
1101
A/D変換部
1102
誤り検出/訂正部
1103
チャネル選択部
1104
フィルター部
1107
ﾃﾞｽｸﾗﾝﾌﾞﾙ部
1108
ﾁｬﾈﾙｷｰ出力部
1120
ﾁｬﾈﾙｷｰ復号部
1109
ﾁｬﾈﾙｷｰ格納部 (Kch)
1117
契約判定部
1118
ﾁｬﾈﾙ情報入力部
1119
ﾁｬﾈﾙｷｰ復号鍵格納部
1115
契約情報復号部
1110
契約情報
認証部
Kh
ﾁｬﾈﾙ契約情報格納部
1116
Km
1114
STID
ﾏｽﾀｰ鍵生成部
1111
ﾏｽﾀｰ鍵格納部 (Km)
1112
受信装置ID格納部
1113
1105
ﾁｬﾈﾙ選択 I/F
受信装置
カードリーダ
2061
カード
P

フロントページの続き

(72)発明者　遠藤　直樹
東京都府中市東芝町１番地　株式会社東芝
府中工場内

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成16年10月14日(2004.10.14)

【公開番号】特開平11-243536
【公開日】平成11年9月7日(1999.9.7)
【出願番号】特願平10-228287
【国際特許分類第７版】
　Ｈ０４Ｎ　7/16
　Ｈ０４Ｈ　1/00
　Ｈ０４Ｌ　9/08
　Ｈ０４Ｌ　9/32
【ＦＩ】
　Ｈ０４Ｎ　7/16　　Ｚ
　Ｈ０４Ｈ　1/00　　Ｆ
　Ｈ０４Ｌ　9/00　６０１Ａ
　Ｈ０４Ｌ　9/00　６７１

【手続補正書】
【提出日】平成15年9月30日(2003.9.30)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、
複数の放送受信装置に共通のマスター鍵と本放送受信装置に一意に設定された識別情報とを格納する格納手段と、
少なくとも前記契約情報と該契約情報に対応した識別情報と、前記暗号化されたコンテンツを復号するためのチャネルキーとを含む暗号化された受信契約情報を受信する第１の受信手段と、
前記第１の受信手段で受信した暗号化された受信契約情報を、前記マスター鍵を利用し、該暗号化された受信契約情報を順次復号する受信契約情報復号手段と、
前記受信契約情報復号手段で復号した受信契約情報のうち、本放送受信装置の有する識別情報に一致する識別情報に対応付けられた契約情報を取得する契約情報取得手段と、
前記契約情報取得手段で取得した該契約情報に基づき、前記コンテンツ情報の視聴の可否を判定する判定手段と、
前記判定手段で視聴可と判定された際に、前記受信契約情報復号手段で復号されたチャネルキーで暗号化されたコンテンツ情報を復号するコンテンツ復号手段とを備えたことを特徴とする放送受信装置。
【請求項２】
前記受信契約情報は、少なくとも前記識別情報を含む第１の受信契約情報と少なくとも前記チャネルキーを含む第２の受信契約情報とからなり、前記受信手段で前記第１の受信契約情報と前記第２の受信契約情報とが受信されたときに、前記コンテンツ復号手段で前記暗号化されたコンテンツ情報を復号することを特徴とする請求項１記載の放送受信装置。
【請求項３】
前記受信契約情報には、前記チャネルキーの一部を含み、前記受信手段は、前記チャネル

キーの他の一部を別途受信することを特徴とする請求項１記載の放送受信装置。
【請求項４】
暗号化されたコンテンツ情報を含む通常放送波を受信する第２の受信手段をさらに具備し、
前記第１の受信手段は、暗号化された前記チャネルキーを復号するためのチャネルキー復号鍵をさらに含む前記暗号化された前記受信契約情報を含む契約放送波を受信し、
前記第１の受信手段で受信した前記暗号化された受信契約情報を前記マスター鍵に基づいて復号して前記チャネルキー復号鍵を取得し、その取得したチャネルキー復号鍵を用いて、前記暗号化チャネルキーを復号することによってチャネルキーを取得し、前記取得した契約情報に基づき、前記コンテンツ情報の視聴の可否を判定することを特徴とする請求項１記載の放送受信装置。
【請求項５】
暗号化されたコンテンツ情報と前記チャネルキーの一部を含む通常放送波を受信する第２の受信手段をさらに具備し、
前記第１の受信手段は、前記チャネルキーの他の一部を含む前記暗号化された受信契約情報を含む契約放送波を受信し、
前記第１の受信手段で受信した前記暗号化された受信契約情報を前記マスター鍵に基づいて復号して前記チャネルキーの他の一部と前記契約情報を取得し、前記第２の受信手段で受信したチャネルキーの一部と前記取得したチャネルキーの他の一部とからチャネルキーを再生し、前記取得した契約情報に基づき、前記コンテンツ情報の視聴の可否を判定することを特徴とする請求項１記載の放送受信装置。
【請求項６】
暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする請求項１記載の放送受信装置。
【請求項７】
前記受信契約情報に含まれるデジタル署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする請求項１記載の放送受信装置。
【請求項８】
内部データをテスト出力するためのテスト制御部を具備し、このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを制御することを特徴とする請求項１記載の放送受信装置。
【請求項９】
暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダを具備したことを特徴とする請求項１記載の放送受信装置。
【請求項１０】
暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコンテンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、
少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と該識別情報に対応し前記放送受信装置ごとの前記契約情報とを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して配信する手段と、
前記暗号化されたコンテンツ情報を復号するためのチャネルキーを配信する手段と、
を具備したことを特徴とする契約管理装置。
【請求項１１】
暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコン

テンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、
少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と該識別情報に対応し、前記放送受信装置ごとの前記契約情報と前記暗号化されたコンテンツ情報を復号するための暗号化されたチャネルキーを復号するためのチャネルキー復号鍵とを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して配信する手段を具備したことを特徴とする契約管理装置。
【請求項１２】
暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコンテンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、
少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と該識別情報に対応し、前記放送受信装置ごとの前記契約情報として前記暗号化されたコンテンツ情報を復号するためのチャネルキーの一部とを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して配信する手段と、
前記チャネルキーの他の一部を配信する手段と、
を具備したことを特徴とする契約管理装置。
【請求項１３】
暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき暗号化されたコンテンツ情報を復号する複数の放送受信装置を管理する契約管理装置であって、
少なくとも前記複数の放送受信装置のそれぞれに一意に設定された識別情報と、該識別情報に対応し、前記放送受信装置ごとの前記契約情報と、前記暗号化されたコンテンツ情報を復号するためのチャネルキーとを含む受信契約情報を前記複数の放送受信装置に共通のマスター鍵に基づいて暗号化して放送配信する手段を具備したことを特徴とする契約管理装置。
【請求項１４】
カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする請求項１０～請求項１３のいずれか１つに記載の契約管理装置。
【請求項１５】
契約に変化の生じた契約者の受信契約情報を選択的に送信することを特徴とする請求項１０～請求項１３のいずれか１つに記載の契約管理装置。
【請求項１６】
前記受信契約情報に含まれる情報の種別に応じた識別子に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする請求項１記載の放送受信装置。
【請求項１７】
前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする請求項１０～請求項１３のいずれか１つに記載の契約管理装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正の内容】
【００１０】
【課題を解決するための手段】
（１）暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき、放送配信される暗号化コンテンツ情報を復号する放送受信装置において、複数の放送受信装置に共通のマスター鍵と本放送受信装置に固有に設定された受信装置ＩＤを持ち、少なくとも前記契約情報と該契約情報に対応した受信装置ＩＤを含む暗号化された受信契約情報を受信したとき、前記マスター鍵を用いて、該暗号化された受信契約情報を順次復号し、該復号された受信契約情報のうち、本放送受信装置の有する受信装置ＩＤに一致する受信装置ＩＤに対応付けられた契約情報を選択して取得し、その取得した契約情報に基づき、暗号化された情報コンテンツを復号するチャネルキーを暗号化されたコンテンツ情報を復号する

ための復号部に送るか否か制御することを特徴とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正の内容】
【００１２】
（２）第２の実施形態（チャネルキーは、受信契約情報とは別途に配布）
請求項１記載の放送受信装置において、前記チャネルキーは別途受信し、前記受信契約情報を受信しない限り、前記チャネルキーは前記復号部に送られることがないように制御することを特徴とする。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正の内容】
【００１３】
（３）第３の実施形態（受信契約情報にチャネルキー復号鍵が含まれる）
上記（１）記載の放送受信装置において、暗号化された前記チャネルキーを別途受信し、この暗号化されたチャネルキーを復号するチャネルキー復号鍵を含む前記受信契約情報を受信しない限り、前記チャネルキーが復号されないよう制御することを特徴とする。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】変更
【補正の内容】
【００１４】
（４）第１の実施形態（受信契約情報にチャネルキーの一部が含まれる）
上記（１）記載の放送受信装置において、前記チャネルキーの一部は別途受信され、前記チャネルキーの他の一部を含む前記受信契約情報を受信しない限り、前記チャネルキーが得られないように制御することを特徴とする。
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正の内容】
【００１５】
（５）第４の実施形態（受信契約情報にチャネルキーが含まれる）
上記（１）記載の放送受信装置において、前記チャネルキーは、前記受信契約情報に含まれて受信され、前記受信契約情報を受信しない限り、前記チャネルキーが得られないものであることを特徴とする。
（６）第２の実施形態（チャネルキーは、受信契約情報とは別途に配布）
上記（１）記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、前記暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、を具備し、前記マスター鍵を用いて、前記第１もしくは第２の受信手段で受信した暗号化されたチャネルキーを復号してチャネルキーを取得するとともに、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記契約情報を取得し、その取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。
【手続補正７】

【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正の内容】
【００１６】
（７）第３の実施形態（受信契約情報にチャネルキー復号鍵が含まれる）
上記（１）記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、前記暗号化されたチャネルキーを復号するためのチャネルキー復号鍵を含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、を具備し、前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記チャネルキー復号鍵を取得し、その取得したチャネルキー復号鍵を用いて、前記第１もしくは第２の受信手段で受信した暗号化チャネルキーを復号することによってチャネルキーを取得し、前記取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】変更
【補正の内容】
【００１７】
（８）第１の実施形態（受信契約情報にチャネルキーの一部が含まれる）
上記（１）記載の放送受信装置において、暗号化された放送コンテンツ情報と前記チャネルキーの一部を含む通常放送波を受信する第１の受信手段と、前記チャネルキーの他の一部を含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段を具備し、前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して前記チャネルキーの他の一部と前記契約情報を取得し、前記第１の受信手段で受信したチャネルキーの一部と前記取得したチャネルキーの他の一部とからチャネルキーを再生し、前記取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報を復号するための復号部に送るか否か制御することを特徴とする。
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
（９）第４の実施形態（受信契約情報にチャネルキーが含まれる）
上記（１）記載の放送受信装置において、暗号化されたコンテンツ情報を含む通常放送波を受信する第１の受信手段と、前記チャネルキーを含む暗号化された受信契約情報を含む契約放送波を受信する第２の受信手段と、を具備し、前記マスター鍵を用いて、前記第２の受信手段で受信した暗号化された受信契約情報を復号して該受信契約情報に含まれる契約情報とチャネルキーを取得し、その取得した契約情報に基づき、前記チャネルキーを暗号化されたコンテンツ情報の復号部に送るか否か制御することを特徴とする。
（１０）上記（１）～（９）記載の放送受信装置において、チャネルキー、マスター鍵の少なくとも一方が変更されることを特徴とする。
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】変更
【補正の内容】

【００１９】
鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。
（１１）上記（１）、（３）、（７）記載の放送受信装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうちの少なくとも１つが変更されることを特徴とする。
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】変更
【補正の内容】
【００２０】
鍵情報に有効期間が定められていることにより、契約期間の管理（契約期間の開始、終了、継続等）が容易に行える。また、コンテンツの不正視聴防止等のセキュリティの向上が図れる。
（１２）上記（１）～（９）記載の放送受信装置において、チャネルキー、マスター鍵の少なくとも一方が変更され、チャネルキー、マスター鍵のそれぞれは、同時に最大２つの鍵を保持することを特徴とする。
（１３）上記（１）～（９）記載の放送受信装置において、チャネルキー、マスター鍵の少なくとも一方が変更され、チャネルキー、マスター鍵のそれぞれにおいて同時に最大２つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。
（１４）上記（１）、（３）、（７）記載の放送受信装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうちの少なくとも一つが変更され、チャネルキー、チャネルキー復号鍵、マスター鍵のそれぞれは、同時に最大２つの鍵を保持することを特徴とする。
（１５）上記（１）、（３）、（７）記載の放送受信装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうちの少なくとも１つが変更され、チャネルキー、チャネルキー復号鍵、マスター鍵のそれぞれは、同時に最大２つの鍵を保持し、鍵変更の際には古い方を更新することを特徴とする。
（１６）上記（１）～（９）記載の放送受信装置において、チャネルキーは、チャネル毎に同時に最大２つ保持することを特徴とする。
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】変更
【補正の内容】
【００２１】
チャネルキーをチャネル毎に最大２つ保持することにより、チャネル切替時であっても（切替元にチャネルの受信契約を行っていれば）、保持している当該チャネルのチャネルキーを暗号化されたコンテンツ情報の復号部に即時的に送ることでチャネル切替の受信状態を良好にできる。
（１７）上記（１）記載の放送受信装置において、暗号化されたコンテンツ情報を復号するための内容の正確性が要求される必須情報（例えば、チャネルキー等の鍵情報、受信契約情報）の誤受信検出のために、それぞれの必須情報に認証子が付加されたデータを受信し、前記認証子とそれが付加された必須情報とを照合し、照合に失敗した場合は当該必須情報を無効にすることを特徴とする。
（１８）上記（１７）記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、その一部であることを特徴とする。

（１９）上記（１７）記載の放送受信装置において、暗号化された必須情報の認証子は、該必須情報を該必須情報で暗号化したもの、あるいは、前記暗号化された必須情報を該必須情報で再暗号化したもの、あるいは、数回再暗号化した情報のうち全部あるいは一部であることを特徴とする。
（２０）上記（１７）記載の放送受信装置において、暗号化されていない必須情報（例えば、マスター鍵シード）の認証子は、該必須情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化したもの、あるいは、それをさらに圧縮したものを用いることを特徴とする。
（２１）上記（１）記載の放送受信装置において、前記受信契約情報に含まれるデジタル署名を検証し、検証により正当性の確認されたデジタル署名を持つ受信契約情報に含まれる契約情報のみを受理することを特徴とする。
（２２）上記（２１）記載の放送受信装置において、受信契約情報に当該放送受信装置に対する契約情報が含まれた時のみ、受信契約情報に含まれるデジタル署名を検証することを特徴とする。
（２３）上記（２１）記載の放送受信装置において、デジタル署名検証用の公開鍵を変更することを特徴とする。
（２４）上記（１）記載の放送受信装置において、内部データ（復号された受信契約情報、放送受信装置内の受信装置ＩＤ格納部に格納されている受信装置ＩＤ）をテスト出力するためのテスト制御部（スキャンパステスト用ラッチ部）を具備し、このテスト制御部は、前記受信契約情報に付加されたテスト用である旨の識別子を確認することにより、あるいは、該受信契約情報に付加されたデジタル署名の正当性を確認することにより、前記内部データをテスト出力するか否かを制御することを制御することを特徴とする。
（２５）上記（２４）記載の放送受信装置において、前記テスト制御部は、暗号化された内部データを出力することを特徴とする。
（２６）上記（１）記載の放送受信装置において、暗号化された受信契約情報を記録したカード型記録媒体から該暗号化された受信契約情報を読み出して本放送受信装置に受信させるカードリーダを具備したことを特徴とする。
（２７）上記（２６）記載の放送受信装置において、前記カードリーダは、有効期間毎に複数の契約情報が記録された磁気カードから、前記複数の契約情報を読み出し、有効期間に応じてそれらの複数の契約情報を使い分けることを特徴とする。
（２８）契約管理装置
暗号化されたコンテンツ情報の復号を制御するための契約情報に基づき放送配信される暗号化コンテンツ情報を復号することにより該コンテンツ情報を受信する複数の放送受信装置を管理する契約管理装置において、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００２２
【補正方法】変更
【補正の内容】
【００２２】
本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。
（２９）第２の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーは暗号化されたコンテンツ情報を復号するための復号部に送られることがないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定さ

れた受信装置ＩＤと該受信装置ＩＤに対応した契約情報を含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャネルキーは前記受信契約情報とは別途配信することを特徴とする。

【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正の内容】
【００２３】
本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３０）第３の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するための暗号化されたチャネルキーが復号されないよう制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応した契約情報と前記暗号化されたチャネルキーを復号するためのチャネルキー復号鍵とを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】変更
【補正の内容】
【００２４】
本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３１）第１の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーが得られないように制御することにより、該契約情報に従ったコンテンツ情報の復号を行う複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと、該受信装置ＩＤに対応した契約情報として前記チャネルキーの一部を含むものとを包含する受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信し、前記チャネルキーの他の一部を別途送信することを特徴とする。

【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】変更
【補正の内容】
【００２５】
本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３２）第４の実施形態の契約管理装置暗号化されたコンテンツ情報の復号を制御するための自装置用の契約情報を受信しない限り、該暗号化された情報コンテンツを復号するためのチャネルキーが得られないように、複数の放送受信装置を管理する契約管理装置であって、少なくとも放送受信装置毎個別に設定された受信装置ＩＤと該受信装置ＩＤに対応

レスた契約情報と前記チャネルキーとを含む受信契約情報を複数の放送受信装置に共通のマスター鍵で暗号化して送信することを特徴とする。

【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】変更
【補正の内容】
【００２６】
本発明によれば、限定受信のための情報を送信できる放送帯域が狭かったり、契約者が予想外に多くなってしまった場合であっても、同程度の安全性を保ちながら限定受信のための情報を各放送受信装置に配信できる。

（３３）上記（２９）～（３０）記載の契約管理装置において、チャネルキーおよびマスター鍵のうち少なくとも１つが予め定められた期間で変更されることを特徴とする。

（３４）上記（２９）～（３２）記載の契約管理装置において、チャネルキーおよびチャネルキー復号鍵およびマスター鍵のうち少なくとも１つが予め定められた期間で変更されることを特徴とする。

（３５）上記（２９）～（３２）記載の契約管理装置において、前受信契約情報に対する認証子を受信契約情報に含めて送信することを特徴とする。

（３６）上記（２９）～（３２）記載の契約管理装置において、前記受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報で前記契約情報を暗号化したもの、もしくは、その一部を用いることを特徴とする。

（３７）上記（２９）～（３２）記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報に含まれる鍵情報を該鍵情報で暗号化したもの、前記暗号化された鍵情報を鍵情報で再暗号化したもの、もしくは数回再暗号化した情報のうち全部もしくは一部を用いることを特徴とする。

（３８）上記（２９）～（３２）記載の契約管理装置において、受信契約情報に対する認証子を受信契約情報に含めて送信し、該認証子として、受信契約情報を必要があればブロック分割し、それぞれのブロックの情報を鍵として当該情報を暗号化し、必要があれば圧縮したものを用いることを特徴とする。

（３９）上記（２９）～（３２）記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信することを特徴とする。

（４０）上記（２９）～（３２）記載の契約管理装置において、受信契約情報に該受信契約情報に対するデジタル署名を付加して送信し、デジタル署名検証用の公開鍵と作成用の秘密鍵のペアを生成する機構を具備し、一定期間で前記デジタル署名用の公開鍵と秘密鍵を変更すると共に、前記デジタル署名検証用の公開鍵を送信することを特徴とする。

（４１）上記（２９）～（３２）記載の契約管理装置において、カード型記録媒体に前記暗号化された受信契約情報を記録する記録手段を具備したことを特徴とする。

（４２）上記（２９）～（３２）記載の契約管理装置において、最近一定期間内に契約の変化の生じた（新規契約を含む）契約者の受信契約情報を選択的に送信することをことを特徴とする。

【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】変更
【補正の内容】
【００２７】
契約の種類（例えば、契約変更、新規契約など）と契約後の経過期間によって、契約情報の放送頻度を変更するようにしてもよい。

（４２－１）上記（２９）～（３２）記載の契約管理装置において、契約の変化の生じた(新規契約を含む）時期により、受信契約情報の送信頻度を変化させることを特徴とする

。
（４３）上記（１）～（９）、（１７）、（２１）、（２４）、（２６）記載の放送受信装置において、前記受信契約情報に含まれる情報の種別に応じた識別子（情報識別子）に基づき、該受信契約情報に対する処理形態を切り替えることを特徴とする。
（４４）上記（２９）～（３２）記載の契約管理装置において、前記受信契約情報を送信すべき契約者の数に応じて、受信契約情報の送信形態を切り替えることを特徴とする。

THIS PAGE LEFT BLANK